

(19) World Intellectual Property Organization  
International Bureau



(43) International Publication Date  
7 December 2000 (07.12.2000)

PCT

(10) International Publication Number  
**WO 00/73106 A1**

(51) International Patent Classification<sup>7</sup>: B60R 25/00,  
25/04

(21) International Application Number: PCT/BE99/00066

(22) International Filing Date: 26 May 1999 (26.05.1999)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant and

(72) Inventor: BREKALO, Berislav [BE/BE]; Pulse Pad 68,  
B-2280 Grobbendonk (BE).

(74) Agents: GEVERS, François et al.; Gevers & Vander  
Haeghen, Rue de Livourne 7, B-1060 Brussels (BE).

(81) Designated States (*national*): AE, AL, AM, AT, AT (util-  
ity model), AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN,

CU, CZ, CZ (utility model), DE, DE (utility model), DK,  
DK (utility model), EE, EE (utility model), ES, FI, FI (util-  
ity model), GB, GD, GE, GH, GM, HR, HU, ID, IL, IN,  
IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV,  
MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU,  
SD, SE, SG, SI, SK, SK (utility model), SL, TJ, TM, TR,  
TT, UA, UG, US, UZ, VN, YU, ZA, ZW.

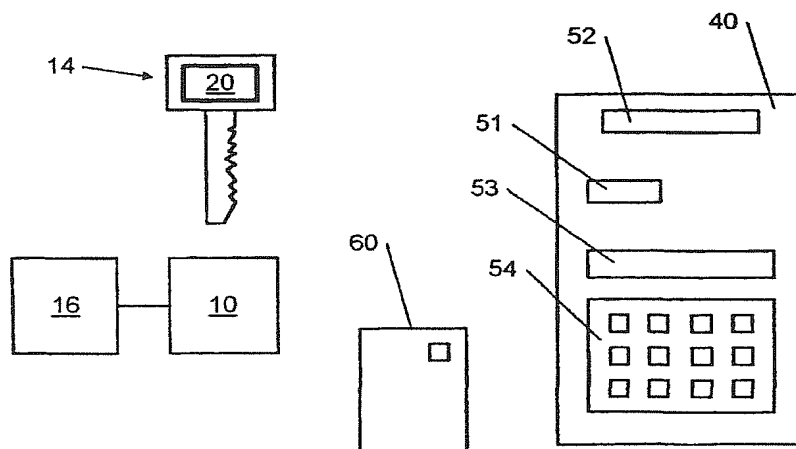
(84) Designated States (*regional*): ARIPO patent (GH, GM,  
KE, LS, MW, SD, SL, SZ, UG, ZW), Eurasian patent (AM,  
AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT,  
BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC,  
NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA,  
GN, GW, ML, MR, NE, SN, TD, TG).

**Published:**

- With international search report.
- With amended claims.

*For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.*

(54) Title: THEFT PROTECTION DEVICE



(57) Abstract: A theft protection device is disclosed for a key operated motorised vehicle having a vehicle operation management system. The theft protection device comprises a key receiving unit connected to said vehicle operation management system; a first key provided for cooperating with said key receiving unit for enabling operation of said vehicle; and a control unit provided for receiving a series of condition parameters, comparing each condition parameter of said series of parameters with a dedicated state value, and generating an inhibit signal when at least one of said condition parameters is met by said dedicated state value, said control unit comprising an output for supplying said inhibit signal to said vehicle. The control unit is provided in said first key. The key receiving unit is provided for receiving said inhibit signal and transmitting said inhibit signal to said vehicle operation management system. The theft protection device further comprises an initialisation unit provided for generating said condition parameters and for supplying said condition parameters to said control unit.

WO 00/73106 A1

**"Theft protection device"**

**BACKGROUND OF THE INVENTION**

The present invention relates to a theft protection device for a key operated motorised vehicle having a vehicle operation management system, said theft protection device comprising: a key receiving unit connected to said vehicle operation management system; a first key provided for cooperating with said key receiving unit for enabling operation of said vehicle; and a control unit provided for receiving a series of condition parameters, comparing each condition parameter of said series of parameters with a dedicated state value, and generating an inhibit signal when at least one of said condition parameters is met by said dedicated state value, said control unit comprising an output for supplying said inhibit signal to said vehicle.

Such a device is known from WO-A-95/13205, wherein the control unit is integrated in the vehicle operation management system. A first key receiving unit, connected to the control system of the vehicle, is provided for receiving the first key and is used to operate the vehicle in a conventional manner. The device further comprises a second key receiving device, connected to the vehicle operation management system. This second key receiving unit is provided for receiving a second key, e.g. a chip card. The second key is provided for determining the condition parameter, which is in particular a time period, during which the vehicle is rendered operable.

The chip card is normally not carried in the vehicle, so that when the condition parameter is met, the operation of the vehicle is

- 2 -

inhibited. This enables to protect the vehicle in case of theft, car jacking or the like.

Before the condition parameter is met, the proprietor of the vehicle may introduce his chip card into the second key receiving device and determine a new condition parameter by means of a user interface, connected to the second key receiving device.

A problem of the known device is that it forms an integral part of the vehicle protection system, thus making it incompatible to existing vehicle operation management systems already installed in the vehicle to be protected. In particular, the control unit needs necessarily to be configured in order to receive signals from the user interface and the chip card, through the intermediary of the second key receiving device, and to generate an inhibit signal for inhibiting the operation of the object.

## SUMMARY OF THE INVENTION

This problem is solved in the device according to the present invention which is characterised in that said control unit is provided in said first key; said key receiving unit is provided for receiving said inhibit signal and transmitting said inhibit signal to said vehicle operation management system; and said theft protection device further comprises an initialisation unit provided for generating said condition parameters and for supplying said condition parameters to said control unit.

By providing that the control unit is provided in the first key, the device according to the invention is compatible with existing vehicle operation management systems provided for receiving a coded signal from the key receiving unit. Under normal circumstances, an "enable" code is transmitted from the key to the vehicle operation management

- 3 -

system. In case the condition parameter is met, the inhibit signal is transmitted instead of the enable code. The control unit can easily be initialised by making use of the initialisation unit. In particular, the device according to the present invention can easily be employed in an existing  
5 transponder system of a vehicle.

In a first preferred embodiment, the control unit comprises:  
a) at least one state machine, each state machine having a first input for receiving a dedicated condition parameter from said series of condition parameters, a second input for receiving said dedicated state value, said  
10 state machine being provided for: i) comparing said dedicated condition parameter with said dedicated state value, ii) generating a first state signal upon establishing that said state value has not met said condition parameter, iii) generating a second state signal upon establishing that s  
said state value has met said condition parameter, said state machine  
15 further comprising an output for transmitting said state signal; b) a logic unit having an input connected to the output of each state machine for receiving said state signals, said logic unit being provided for generating said inhibit signal upon establishing that at least one of said second signals correspond to said second signal, said logic unit comprising an  
20 output for supplying said inhibit signal to said vehicle operation management system. This enables to check with different parameters if the operation of the vehicle may be enabled.

In a second preferred embodiment, said initialisation unit comprises user interface for establishing said condition parameters. This  
25 enables a user of the theft protection device to determine himself the condition parameters to be supplied to the control unit.

In a third preferred embodiment, the device further comprises a second key, in particular a chip card, dedicated to said first key, and said initialisation unit comprises second key receiving means

- 4 -

for receiving said second key, and upon receipt of said second key for enabling supplying said condition parameters to said control unit. On the one hand, it enhances the security of the initialising unit, since condition parameters will only be supplied by the initialisation unit if the second

5 key is cooperating with the second key receiving means. On the other hand, a same initialisation unit can be used for several first keys. For each of the first keys, a dedicated second key must be used for supplying the condition parameters. In particular, the initialisation units could be foreseen in predetermined locations, enabling the proprietor of

10 the vehicle to "charge" his key with new condition parameters.

In a fourth preferred embodiment, said initialisation unit is provided for enabling said supply of condition parameters after a predetermined period of time. This could for example be achieved by providing that the user must enter two codes. After entering a first code,

15 he has to wait a predetermined period of time, for example 30 minutes, before entering a second code. Only after entering and validating the second code, the condition parameters can be supplied to the control unit of the first key.

In a fifth preferred embodiment, one of said condition

20 parameters indicates a time period during which said vehicle is operable. This type of condition parameters may be useful for vehicle renters, on the one hand, since the car renter could set as condition parameters the period of time the car is rented, with possibly an extra time period. On the other hand, car insurers could set a limited period of time corresponding

25 to the validity period of the insurance. In case of car jacking, the vehicle could also have a limited period of time during which the vehicle is operable, making it unattractive for the car jacker.

In a sixth preferred embodiment, one of said condition parameters indicates a number of allowed ignitions for said vehicle. This

- 5 -

type of condition parameters is useful for the car owner, since in case of car jacking, the criminal could use the car for a limited number of ignitions. After the condition parameter is met, the operation of the engine and other vital parts is inhibited.

5                   The present invention also relates to a first key as defined in any one of the claims 1 to 10 to be used in a theft protection device.

                  The present invention further relates to an initialisation unit as defined in any one of the claims 1 to 10 to be used in a theft protection device.

10

#### BRIEF DESCRIPTION OF THE DRAWINGS

                  Figure 1 illustrates a preferred embodiment of a theft protection device according to the present invention.

15                   Figure 2 is a block diagram of the internal circuitry of the device of Figure 1.

#### DETAILED DESCRIPTION OF THE INVENTION

                  Keys comprising a code to be transmitted to the key receiving unit are well known in the art as transponder based anti theft systems. In order to activate the vital parts of the vehicle, it is necessary to use the key comprising the dedicated code. Such a provision has been effective to reduce significantly the theft of vehicles. However, it is not effective for preventing car jacking, since the criminal obtains the vehicle together with the key by menacing the driver. Once the criminal is in possession of the car with the coded key, the vehicle is permanently operable by the criminal, since the correct code is supplied to the vehicle operation management system. The weakness of the current transponder system is that the key will operate permanently.

20

25

- 6 -

Current anti car jacking systems are implemented as additional mechanisms that interact with the vehicle operation management system. They don't use the features of the transponder key, but introduce additional transmitters, codes and keys. For example, use  
5 is made of a radio or GSM receiver, hidden in the vehicle. A drawback of these systems is that additional interference could occur with the electronics of the vehicle, that they are only effective during a limited period of time, i.e. until the criminal finds and disables the additional features, and that they can be made ineffective when the vehicle is  
10 moved to a place where no radio reception is available. The interference problem can not be solved generically, since it is dependent from the electronics used in the car.

The system according to the present invention is in particular an extension of the transponder based anti theft systems  
15 installed on many types of vehicles. As will be explained further in detail, the theft protection device according to the present invention essentially consists in providing a condition parameter which will enable operation of the vehicle according to a predetermined parameter, for example a limited number of ignitions, a limited period of time, .... A combination of  
20 several parameters is preferred.

Referring to figure 1, the theft protection device according to the present invention comprises a key receiving unit 10, cooperating with the operation management system 16 of the vehicle, on the one hand, and with a control unit 20, on the other hand. The vehicle  
25 operation management system is known as such and will therefore not be described in detail.

An initialisation unit 40 is further provided for generating and supplying condition parameters to the control unit 20, as explained further in detail. The initialisation unit comprises a slot 51 for receiving a

- 7 -

first key 14, a slot 52 for receiving a chip card 60 dedicated to the first key 14 and a user interface with a display 53 and a keyboard 54.

According to the invention, the control unit 20 is provided in the first key 14. As illustrated in Figure 1, the first key may be a conventional key which is used for starting the engine of the vehicle. It is to be understood that the first key could also be a probe with a printed circuit board to be inserted in a slot of the key receiving unit for enabling operation of the starting circuit. An additional conventional key is then used for starting the vehicle. It is also conceivable that the first key consists in a chip card transmitting with transponder technology the required codes to enable operation of the vehicle. The vehicle itself could be started in this case with a switch provided in the vehicle, which will only be operable if the driver carries the chip card with the required code.

The control unit is provided for receiving a series of condition parameters supplied by the initialisation unit. Further, the control unit is provided for comparing each condition parameter of the series of parameters with a dedicated state value, and generating an inhibit signal when at least one of the condition parameters is met by the dedicated state value. The control unit comprises an output for supplying the inhibit signal to the key receiving device of the vehicle. The control unit further comprises a battery for supplying power to the clock.

The key receiving unit 10 is provided for receiving the inhibit signal and transmitting the inhibit signal to the vehicle operation management system 16.

Figure 2 shows in detail an internal circuitry of the key receiving unit 10, the control unit 20 and the initialisation unit 40 in a preferred embodiment according to the present invention.



- 8 -

The key receiving unit 10 comprises a receiver 11 and a transmitter 12. The transmitter 12 is provided for supplying a challenge code to the control unit 20. The challenge code is for example a request to transmit the key code from the key to the key receiving unit, as known from existing transponder based theft protection systems. The receiver 11 is provided for receiving a response code supplied by the control unit and transmitting the received response code to the vehicle operation management system. In particular, the transmission between the key receiving unit and the control unit in the first key occurs by means of electromagnetic signals.

Control unit 20 comprises a transmitter 21 having an input 211 connected to an output 232 of a logic unit 23 and an output 212 provided for transmitting the response code to the receiver 11. A receiver 22 has an input 221 for receiving the challenge code from the transmitter 12 and an output 222 connected to an input 231 of the logic unit 23. The logic unit further comprises two further inputs 233 and 234, to each of which a state machine 30, 31 is connected.

A memory 28 is connected to the logic unit 23. The memory, in particular a ROM, is provided for holding a code uniquely identifying the vehicle. Preferably, the code also identifies the first key. It is to be understood that a same vehicle could be made operable with two or more keys, each having an own identifier. Consequently, multiple keys could be linked to one vehicle identifier.

An I/O interface 29 comprises outputs 292, 293 and 294, respectively connected to corresponding inputs 235, 302 and 312 of the logic unit 23 and the state machines 30 and 31. State machine 30 further comprises an input 301 connected to output 223 from the receiver. State machine 31 further comprises an input 311 connected to an output from clock 32 provided in the control unit 20. The state machines are in

- 9 -

particular counters, provided for counting to a threshold value supplied by the I/O interface and supplying a first signal to the logic unit when the threshold value is not reached and a second value when the threshold value is reached.

5                   The I/O interface 29 comprises an input 291 connected to an output 273 of a message validation unit 27. The message validation unit 27 is further connected to a serial interface 24 through in/output 271. The serial interface 24 is further connected to a transmitter 25 and a receiver 26. Output 282 from memory 28 is connected to input 243 from  
10                   serial interface 24 for supplying the key ID to the serial interface. This is required to perform the decryption.

                  The initialisation unit 40 comprises a receiver 41 and a transmitter 42 provided for communicating with the control unit. Such as with the key receiving unit 10, the communication between the  
15                   initialisation unit 40 and the control unit 20 can occur by means of electromagnetic signals. The transmitter 41 and receiver 42 are connected to an encryption/decryption unit 43, which is in turn connected to state machine programming unit master 44. State machine programming unit master is further connected through a bus 45 to a RAM  
20                   46, a ROM 47, a microprocessor 48, a chip card reader 49 and a user interface 50.

                  The second key 60, in particular a chip card, is dedicated to the first key. This signifies that the first key can only be initialised using the unique dedicated chip card. If multiple keys are issued for a same  
25                   vehicle, each key will have its dedicated chip card.

                  The chip card contains an algorithm that identifies the code in memory 28 uniquely identifying the vehicle and the first key. Preferably, the chip card 60 further contains additional algorithms for secret PIN codes to be used when using the initialisation unit.

- 10 -

For initialising and "charging" the control unit 20 in the first key 14, use is made of the initialisation unit 40 and preferably also the second key 60. The initialisation unit is used by the car owner each time he wishes to reset the condition parameters to be supplied to the control unit of the first key. This unit and the chip card will, under normal circumstances, be held at a safe place, for example at the office. It is only brought home by the car owner when recharging is necessary. The first key 14 and the chip card 60 are inserted in their respective slots 51 and 52.

10           The user will introduce the condition parameters to be transmitted to the control unit. In particular, these condition parameters indicate a time limit of the key validity, for example 20 days, and a number of ignitions of the vehicle, for example 25.

15           The user will be requested to input a first PIN code dedicated to the chip card. A validation of the chip card algorithm to check the correctness of the first PIN code is performed by the initialisation unit 40.

20           When the correct code is introduced, the initialisation unit is held in a hold mode during a predetermined period of time, for example 30 minutes, during which both the first key and the chip card must remain inserted in the initialisation unit. This provision is effective to limit the phenomena of "home jacking", whereby the criminal forces the vehicle owner to furnish the key. In case he has to wait 30 minutes before the condition parameters are transmitted to the control unit, the criminal will  
25           be further discouraged.

          Preferably, a second PIN code is input after that predetermined period of time. After checking the correctness of the second PIN code, the condition parameters introduced by the user are passed by the state machine programming unit master 44, encrypted by

- 11 -

the encryption/decryption unit 43 and transmitted through transmitter 42 to the receiver 26 from the control unit 20. When the owner is threaten, he can input a fake (one time usable code), enabling the vehicle to operate for example during one day and 10 ignitions. When at least one  
5 of these parameters is expired, the chip card and key combination must be re-enabled by a code provided by an official organism, e.g. the insurance company. This will further discourage the home-jacker, since he is almost sure that he can only get a vehicle operable for a restricted time, for example one day.

10 According to an alternative, transmission between the initialisation unit and the control unit is simply enabled after the predetermined period of time, without having to introduce a second PIN code.

The encrypted condition parameters are received by  
15 receiver 26 and are transmitted to the serial interface 24. In the interface 24, the parameters are decrypted. The integrity of the received parameters is checked at the message validation unit, which performs in particular a message checksum. The encryption/decryption process enhances security when data is transmitted between the control unit and  
20 the initialisation unit.

The transmitter 25 is provided for ensuring handshaking in the encryption protocol and could additionally transmit the status of the state machines from the control unit to the initialisation unit. The latter allows to display on the initialisation unit the status of the different  
25 parameters.

The I/O interface, which is in particular an n-bit register, processes the received condition parameters and transmits each condition parameter to the dedicated state machine. In the given example, the parameter indicating 25 ignitions is transmitted to state

- 12 -

machine 30 where a threshold value is set to 25. The parameter indicating a validity of 20 days (or 1.728.000 seconds) is transmitted to state machine 31, where a threshold value is set to 1.728.000.

5 When introducing the first key 14 in the key receiving unit 10 of the vehicle. A challenge code is supplied from the vehicle operation management system 16 and transmitted through transmitter 12 to the control unit receiver 22. This challenge code comprises in particular a request for supplying the vehicle and key identifier from the control unit to the key receiving unit.

10 Upon receipt of the challenge code, a signal is transmitted from receiver 22 to the logic unit 23, triggering the logic unit for retrieving the code from the memory 28. In state machine 30, where the threshold value is for example set to 25 ignitions, there is checked if the number of ignitions (performed with this particular key) since the last initialisation is  
15 less than or equal to the threshold value. This is in particular achieved as follows: each time the logic unit is challenged, in particular when the vehicle is started, a pulse is transmitted from the vehicle operation management system 16 to the control unit.

20 A pulse is then transmitted from receiver 22 to state machine 30. In the given example, where the threshold value has been set to 25, the counter has initially as value 25. Each time a signal is transmitted from the receiver to the state machine 30, the counter value is decremented with one unity.

25 As long as the counter value does not reach the value 0, this signifies that the condition parameter is not met. In that case, a first signal, is transmitted from the state machine 30 to the logic unit 23. If the counter value is 0, this signifies that the number of ignitions has reached the condition set by the user. This will cause a second signal to be generated at the state machine 30, which will be transmitted to the logic

- 13 -

unit. This transmitted signal generates a wrong response, resulting in failure of the engine to engage.

5 In the given example, the condition parameter is 25, since 25 ignitions are allowed before the recharging the key. The dedicated state value is the number of ignitions, thus the number of pulses received the receiver, since the last time the condition parameters have been supplied to the control unit. When the number of ignitions meets the conditions parameter, i.e. when the number of ignitions is equal to 25, an inhibit signal is generated.

10 In the state machine 31, there is checked whether or not a time limit, set by the user, is reached. The operation is similar to the state machine 30. In this case, a pulse is supplied by clock 32 to the state machine 31, for example every second. The counter value in state machine 31 is decremented each second with one unity.

15 In the given example, the condition parameter is a time limit equal to 1.728.000 seconds, since 20 days are allowed before the recharging the key. The dedicated state value is the time period, thus the number of pulses received from the clock, since the last time the condition parameters have been supplied to the control unit. When the time limit meets the conditions parameter, i.e. when the time lapsed since the last recharging reaches 20 days, an inhibit signal is generated.

20 When the signals transmitted from the state machines 30, 31 to the logic unit 23 are both first signals, a correct code is transmitted from the logic unit 23 to the key receiving unit 10. This will enable operation of the vehicle. When at least one the signals transmitted from the state machines to the logic unit is a second signals, indicating thus that one of the conditions has been met, an inhibit signal will be generated by the logic unit and transmitted from the logic unit to the key receiving unit. This will inhibit operation of the vehicle.

- 14 -

The inhibit signal is for example an interference signal which is transmitted to the vehicle operation management system. It is to be understood that the transmission of an inhibit signal could also signify that no signal (or a signal having a value low) is transmitted.

5           The operation of the vehicle may be inhibited in several ways, for example : disabling the starting circuit, disabling the fuel supply, .... It is also conceivable that the operation of the vehicle is disabled after a predetermined period of time. This enables the user, in case he forgot to "charge" his key, to rejoin his home where his  
10           initialisation unit and second key are located.

          The described device is thus efficient for discouraging car jacking criminals but is not limited for this purpose. This device could conceivably be required by insurance companies, wherein a time limit, for example 1 year, is determined by the insurance company for  
15           enforcing payment of the insurance premium. A combination of both is also conceivable: the device could in that case comprise two state machines identifying a time limit, one of which can be set by the vehicle owner and the other one by the insurance company. The second key could in that case have an upper limit on its validity. This can be  
20           implemented by limiting the number of days, for example 40 days, during which the second key 60 can charge with the given PIN codes. In order to perform additional charging, the owner must obtain a new set of PIN codes from his insurance (after verification that the vehicle was not reported stolen) or car rental company. An alternative could be that the  
25           owner gets a new chip-card each time he gets its insurance card.

          Other state machines checking other types of conditions parameters could be used in addition or instead of the described state machines, for example maximum driving distance, maximum geographic distance from owners house (this requires a GPS in the vehicle). These

- 15 -

new parameters can be passed by the vehicle operation management system to the logic unit and the additional state machines. In that case, the logic unit 23 could be challenged not only when starting the vehicle, but more generally each time a pulse is transmitted from the vehicle operation management system to the control unit 20.

A warning signal, indicating that one of the conditions is almost met, could conceivably be generated by the control unit to alert the car owner that he should charge his key soon.

The encryption/decryption process is in particular performed as follows. During "charging" the first key 14, the initialisation unit 40 and the control unit 20

During the "charging" of the key, 40 and 20 perform a dialogue. This dialogue is encrypted/decrypted using encryption/decryption unit 43 and interface 24. The encryption and decryption parameters are controlled by the second key 60 in the initialisation unit 40 (in particular enabled by PIN code) and the memory 28 in the control unit 20. If the second key 60 does not is not dedicated to the control unit 20 of the first key 14, no dialogue can take place and the control unit 20 can not be "charged".

The I/O interfaces 44 and 29 dialogue together using messages of fixed length, for example 8 bytes. A possible message format could be :

BYTE 1 : identification of state machine that gets new value (e.g. 30 or 31)  
BYTE 2 : bits 40 .. 47 of new value of the condition parameter  
BYTE 3 : bits 32 .. 39 of new value of the condition parameter  
BYTE 4 : bits 24 .. 31 of new value of the condition parameter  
BYTE 5 : bits 16 .. 23 of new value of the condition parameter  
BYTE 6 : bits 8 .. 15 of new value of the condition parameter



- 16 -

BYTE 7 : bits 0 .. 7 of new value of the condition parameter

BYTE 8 : sum of BYTE 1 to 7 modulo 255

5 It should further be noted that the control unit could be built with discrete components or partially or entirely integrated in a chip. In particular, the elements 23, 24 and 27 to 32 could be integrated in one chip. These techniques of integration are known as such and will therefore not be described in detail.

#### PARTS LIST

10	10	key receiving unit
	11	receiver
	12	transmitter
	14	first key
	16	vehicle operation management system
15	20	control unit in key
	21	transmitter
	22	receiver
	23	logic unit
	24	serial interface
20	25	transmitter
	26	receiver
	27	message validation unit
	28	memory (ROM containing vehicle ID and first key ID)
	29	I/O interface (state machine programming unit slave)
25	30	state machine
	31	state machine
	32	clock
	40	initialisation unit

- 17 -

	41	receiver
	42	transmitter
	43	encryption / decryption unit
	44	I/O interface (state machine programming unit master)
5	45	bus
	46	RAM
	47	ROM
	48	micro processor
	49	chip card reader
10	50	user interface
	51	slot for first key
	52	slot for chip card
	53	display
	54	keyboard
15	60	second key, e.g. a chip card

- 18 -

### CLAIMS

1. A theft protection device for a key operated motorised vehicle having a vehicle operation management system, said theft protection device comprising:
  - 5 a) a key receiving unit connected to said vehicle operation management system;
  - b) a first key provided for cooperating with said key receiving unit for enabling operation of said vehicle; and
  - 10 c) a control unit provided for receiving a series of condition parameters, comparing each condition parameter of said series of parameters with a dedicated state value, and generating an inhibit signal when at least one of said condition parameters is met by said dedicated state value, said control unit comprising an output for supplying said inhibit signal to said vehicle,
  - 15 characterised in that
  - d) said control unit is provided in said first key;
  - e) said key receiving unit is provided for receiving said inhibit signal and transmitting said inhibit signal to said vehicle operation management system; and
  - 20 f) said theft protection device further comprises an initialisation unit provided for generating said condition parameters and for supplying said condition parameters to said control unit.
2. The theft protection device of claim 1, wherein the control unit comprises:
  - 25 a) at least one state machine, each state machine having a first input for receiving a dedicated condition parameter from said series of condition parameters, a second input for receiving said dedicated state value, said state machine being provided for:

- 19 -

- i) comparing said dedicated condition parameter with said dedicated state value,
  - ii) generating a first state signal upon establishing that said state value has not met said condition parameter,
  - 5      iii) generating a second state signal upon establishing that said state value has met said condition parameter,
- said state machine further comprising an output for transmitting said state signal;
- 10      b) a logic unit having an input connected to the output of each state machine for receiving said state signals, said logic unit being provided for generating said inhibit signal upon establishing that at least one of said second signals correspond to said second signal, said logic unit comprising an output for supplying said inhibit signal to said vehicle operation management system.
- 15      3. The theft protection device of claim 2, wherein
  - a) said first key comprises a code receiving unit for receiving a challenge code from said key receiving unit, said code receiving unit comprising an output connected to the logic unit for transmitting said challenge code to said logic unit, and
  - 20      b) said logic unit comprises a code transmitting unit for transmitting said inhibit signal to said key receiving unit.
- 4. The theft protection device of claim 3, wherein the code receiving unit comprises a further output connected to the second input of one of said state machines.
- 25      5. The theft protection device according to any one of the preceding claims, wherein said initialisation unit comprises user interface for establishing said condition parameters.
- 6. The theft protection device according to any one of the preceding claims, further comprising a second key, in particular a chip card,

- 20 -

dedicated to said first key, and said initialisation unit comprises second key receiving means for receiving said second key, and upon receipt of said second key for enabling supplying said condition parameters to said control unit.

- 5      7. The theft protection device according to claim 6, wherein the second key has a validity parameter indicating a validity period during which said second key enables said supplying of condition parameters.
- 10      8. The theft protection device according to claim 6 or 7, wherein said initialisation unit is provided for enabling said supply of condition parameters after a predetermined period of time.
9. The theft protection device according to any one of the preceding claims, wherein one of said condition parameters indicates a time period during which said vehicle is operable.
- 15      10. The theft protection device according to any one of the preceding claims, wherein one of said condition parameters indicates a number of allowed ignitions for said vehicle.
11. The theft protection device according to any one of the preceding claims, further comprising warning means, connected to said control unit for warning said user is when at least one of said condition parameters is almost met.
- 20      12. A first key as claimed in any one of the preceding claims to be used in a theft protection device.
13. An initialisation unit as claimed in any one of the claims 1 to 11 to be used in a theft protection device.
- 25

**AMENDED CLAIMS**

[received by the International Bureau on 08 August 2000 (08.08.00);  
original claims 1-13 replaced by new claims 1-12 (3 pages)]

1. A theft protection device for a key operated motorised vehicle having a vehicle operation management system, said theft protection device comprising:
  - 5 a) a key receiving unit connected to said vehicle operation management system;
  - b) a first key provided for cooperating with said key receiving unit for enabling operation of said vehicle; and
  - 10 c) a control unit provided for receiving a series of condition parameters, comparing each condition parameter of said series of parameters with a dedicated state value, and generating an inhibit signal when at least one of said condition parameters is met by said dedicated state value, said control unit comprising an output for supplying said inhibit signal to said vehicle,
  - 15 wherein
  - d) said control unit is provided in said first key;
  - e) said key receiving unit is provided for receiving said inhibit signal and transmitting said inhibit signal to said vehicle operation management system; and
  - 20 f) said theft protection device further comprises an initialisation unit provided for generating said condition parameters and for supplying said condition parameters to said control unit
- 25 characterised in that said theft protection device further comprises a second key, in particular a chip card, dedicated to said first key, and said initialisation unit comprises second key receiving means for receiving said second key, and upon receipt of said second key for enabling supplying said condition parameters to said control unit.

2. The theft protection device of claim 1, wherein the control unit comprises:

a) at least one state machine, each state machine having a first input for receiving a dedicated condition parameter from said series of condition parameters, a second input for receiving said dedicated state value, said state machine being provided for:

i) comparing said dedicated condition parameter with said dedicated state value,

ii) generating a first state signal upon establishing that said state value has not met said condition parameter,

iii) generating a second state signal upon establishing that said state value has met said condition parameter,

said state machine further comprising an output for transmitting said state signal;

b) a logic unit having an input connected to the output of each state machine for receiving said state signals, said logic unit being provided for generating said inhibit signal upon establishing that at least one of said second signals correspond to said second signal, said logic unit comprising an output for supplying said inhibit signal to said vehicle operation management system.

3. The theft protection device of claim 2, wherein

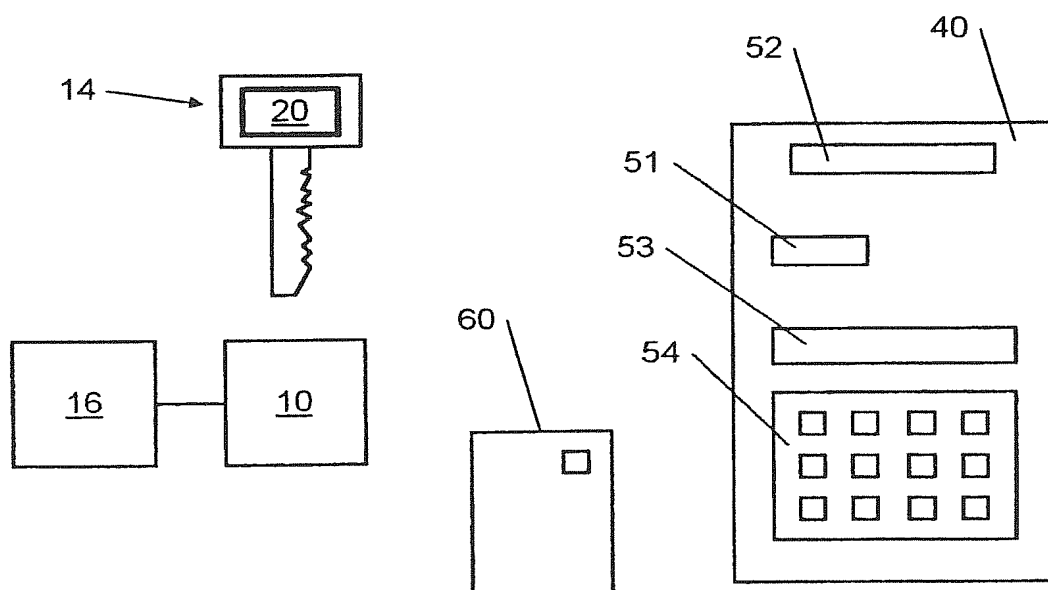
a) said first key comprises a code receiving unit for receiving a challenge code from said key receiving unit, said code receiving unit comprising an output connected to the logic unit for transmitting said challenge code to said logic unit, and

b) said logic unit comprises a code transmitting unit for transmitting said inhibit signal to said key receiving unit.

4. The theft protection device of claim 3, wherein the code receiving unit comprises a further output connected to the second input of one of said state machines.
- 5 5. The theft protection device according to any one of the preceding claims, wherein said initialisation unit comprises user interface for establishing said condition parameters.
6. The theft protection device according to claim any one of the preceding claims, wherein the second key has a validity parameter indicating a validity period during which said second key enables  
10 said supplying of condition parameters.
7. The theft protection device according to any one of the preceding claims, wherein said initialisation unit is provided for enabling said supply of condition parameters after a predetermined period of time.
- 15 8. The theft protection device according to any one of the preceding claims, wherein one of said condition parameters indicates a time period during which said vehicle is operable.
9. The theft protection device according to any one of the preceding claims, wherein one of said condition parameters indicates a  
20 number of allowed ignitions for said vehicle.
10. The theft protection device according to any one of the preceding claims, further comprising warning means, connected to said control unit for warning said user is when at least one of said condition parameters is almost met.
- 25 11. A first key as claimed in any one of the preceding claims to be used in a theft protection device.
12. An initialisation unit as claimed in any one of the claims 1 to 10 to be used in a theft protection device.



1/2

***Fig. 1***

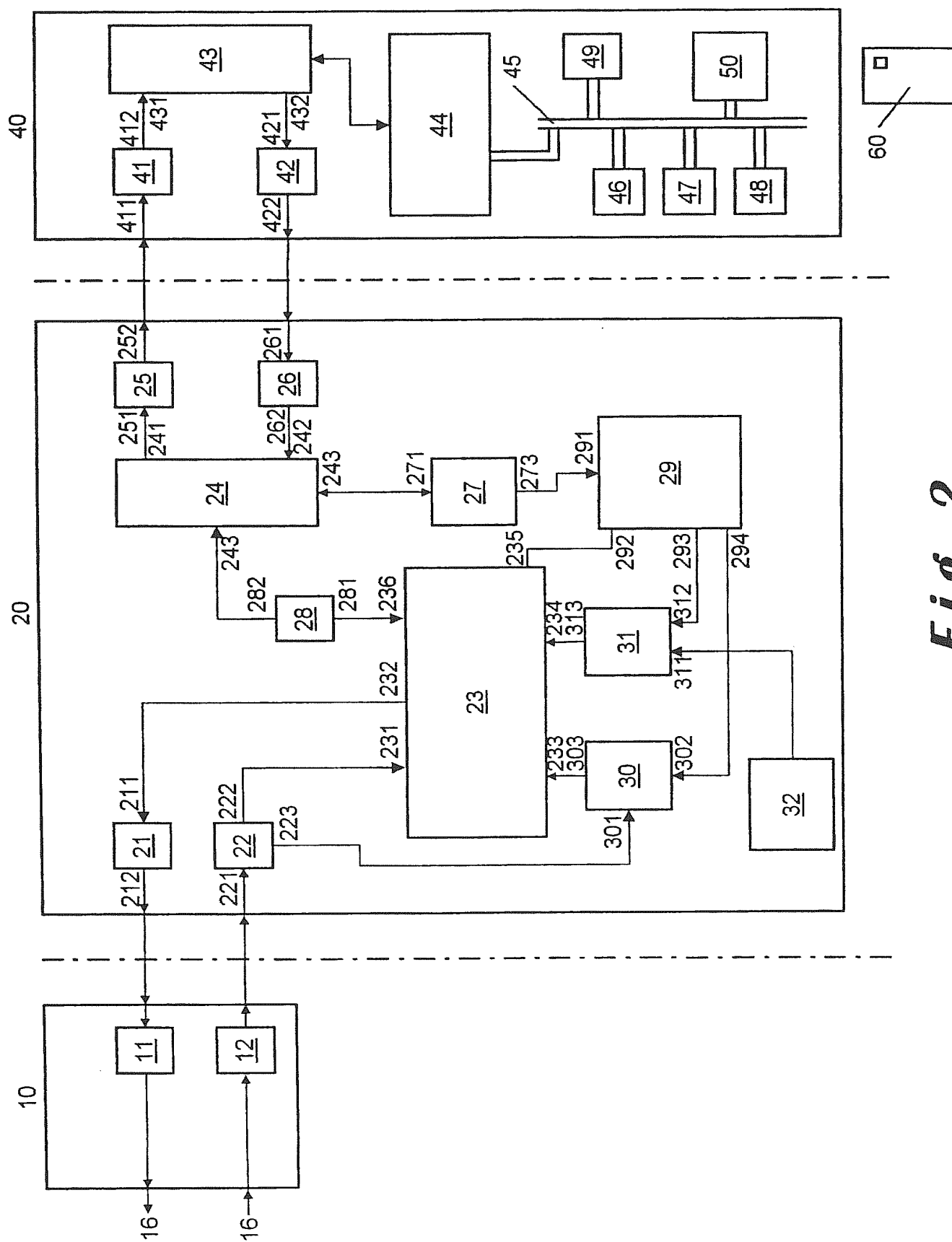


Fig. 2

## INTERNATIONAL SEARCH REPORT

International Application No

PCT/BE 99/00066

## A. CLASSIFICATION OF SUBJECT MATTER

IPC 7 B60R25/00 B60R25/04

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 7 B60R

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category <sup>a</sup>	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
E	DE 197 53 401 A (MARQUARDT GMBH) 10 June 1999 (1999-06-10) column 2, line 68 -column 4, line 18 column 5, line 23 - line 26 figures 1-3 ---	1,9-13
X	DE 196 12 026 A (MARQUARDT GMBH) 2 October 1997 (1997-10-02) column 1, line 5 -column 2, line 18 claim 6 figures 1-4 ----- -/--	1,5,9-13

☒ Further documents are listed in the continuation of box C.☒ Patent family members are listed in annex.<sup>a</sup> Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&amp;" document member of the same patent family

Date of the actual completion of the international search

11 February 2000

Date of mailing of the international search report

17/02/2000

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2  
NL - 2280 HV Rijswijk  
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,  
Fax: (+31-70) 340-3016

Authorized officer

Billen, K

## INTERNATIONAL SEARCH REPORT

International Application No

PCT/BE 99/00066

## C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	DE 195 32 067 C (DAIMLER BENZ AG) 24 October 1996 (1996-10-24)	1,9,10
A	column 1, line 15 - line 19 column 3, line 1 - line 7 column 4, line 32 - line 36 column 5, line 15 - line 21 column 6, line 6 - line 46 column 7, line 1 - line 9 column 11, line 2 -column 12, line 22 figures 1,2 -----	2,3,8
A	DE 195 32 744 A (TELEFUNKEN MICROELECTRON) 6 March 1997 (1997-03-06) column 1, line 10 -column 2, line 18 column 3, line 25 -column 4, line 40 -----	1,6,7, 9-13

# INTERNATIONAL SEARCH REPORT

Information on patent family members

Int. onal Application No

PCT/BE 99/00066

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
DE 19753401 A	10-06-1999	NONE	
DE 19612026 A	02-10-1997	NONE	
DE 19532067 C	24-10-1996	EP 0788946 A	13-08-1997
		JP 2876469 B	31-03-1999
		JP 9152970 A	10-06-1997
		US 5838251 A	17-11-1998
DE 19532744 A	06-03-1997	NONE	





<p>(51) Internationale Patentklassifikation <sup>7</sup> : <b>B60R 25/04</b></p>	<b>A1</b>	<p>(11) Internationale Veröffentlichungsnummer: <b>WO 00/48873</b></p> <p>(43) Internationales Veröffentlichungsdatum: 24. August 2000 (24.08.00)</p>
<div style="display: flex; justify-content: space-between;"> <div style="width: 48%; vertical-align: top;"> <p>(21) Internationales Aktenzeichen: PCT/AT00/00031</p> <p>(22) Internationales Anmeldedatum: 9. Februar 2000 (09.02.00)</p> <p>(30) Prioritätsdaten: A 280/99 19. Februar 1999 (19.02.99) AT</p> <p>(71) Anmelder (für alle Bestimmungsstaaten ausser US): INTER- PAN EXPORT – IMPORT MAREK &amp; CO. [AT/AT]; Un- tere Weissgerberstrasse 17, A-1030 Wien (AT).</p> <p>(72) Erfinder; und (75) Erfinder/Anmelder (nur für US): MAREK, Thomas, M. [AT/AT]; Radetzkystasse 13/16, A-1030 Wien (AT).</p> <p>(74) Anwalt: GIBLER, Ferdinand; Dorotheergasse 7, A-1010 Wien (AT).</p> </div> <div style="width: 48%; vertical-align: top;"> <p>(81) Bestimmungsstaaten: AE, AL, AM, AT, AT (Ge- brauchsmuster), AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, CZ (Gebrauchsmuster), DE, DE (Gebrauchsmuster), DK, DK (Gebrauchsmuster), DM, EE, EE (Gebrauchsmuster), ES, FI, FI (Gebrauchsmuster), GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KR (Gebrauchsmuster), KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SK (Gebrauchsmuster), SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO Patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), eurasisches Patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI Patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).</p> <p>Veröffentlicht <i>Mit internationalem Recherchenbericht.</i></p> </div> </div>		

(54) Title: ANTI-THEFT SYSTEM

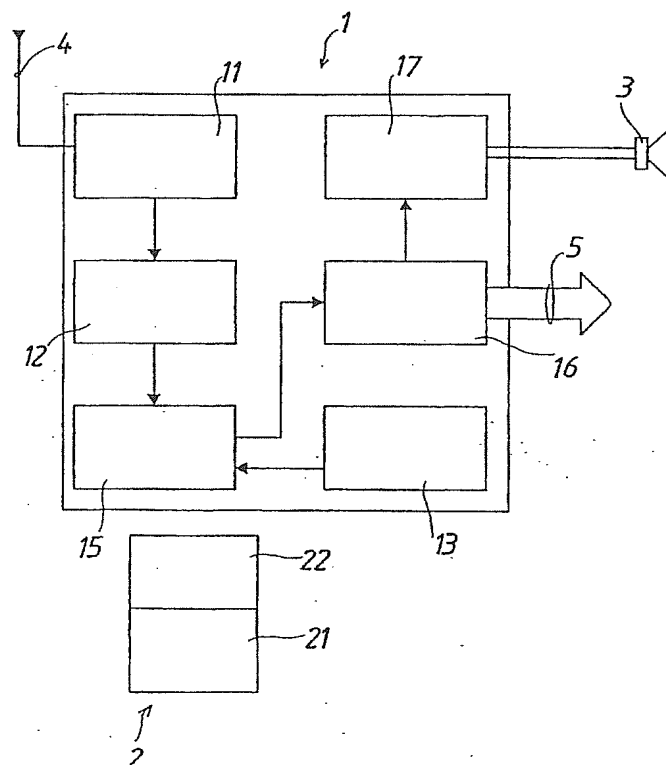
(54) Bezeichnung: EINRICHTUNG ZUR DIEBSTAHL SICHERUNG

(57) Abstract

The invention relates to an anti-theft system of a motor vehicle comprising a device for deactivating the vehicle (34, 35) and comprising a theft detection device (1, 2) via which an unauthorized initial operation of the motor vehicle can be determined, and the deactivation device (34, 35) can be actuated. The deactivation device (34, 35) is connected to a time-delay unit which controls said deactivation device and which triggers the deactivation of the vehicle after a predetermined time span has elapsed after unauthorized initial operation.

(57) Zusammenfassung

Einrichtung zur Diebstahlsicherung eines Kraftfahrzeuges mit einer Vorrichtung zur Deaktivierung des Fahrzeuges (34, 35) und einer Diebstahl-Detektionsvorrichtung (1, 2), über welche eine unautorisierte Inbetriebnahme des Kraftfahrzeuges feststellbar und die Deaktivierungsvorrichtung (34, 35) betätigbar ist, wobei die Deaktivierungsvorrichtung (34, 35) mit einer diese steuernden Zeitverzögerungseinheit verbunden ist, welche die Deaktivierung des Fahrzeuges erst nach Ablauf einer vorbestimmbaren Zeitspanne ab dem Zeitpunkt der unautorisierten Inbetriebnahme auslöst.



### LEDIGLICH ZUR INFORMATION

Codes zur Identifizierung von PCT-Vertragsstaaten auf den Kopfbögen der Schriften, die internationale Anmeldungen gemäss dem PCT veröffentlichen.

AL	Albanien	ES	Spanien	LS	Lesotho	SI	Slowenien
AM	Armenien	FI	Finnland	LT	Litauen	SK	Slowakei
AT	Österreich	FR	Frankreich	LU	Luxemburg	SN	Senegal
AU	Australien	GA	Gabun	LV	Lettland	SZ	Swasiland
AZ	Aserbaidshan	GB	Vereinigtes Königreich	MC	Monaco	TD	Tschad
BA	Bosnien-Herzegowina	GE	Georgien	MD	Republik Moldau	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagaskar	TJ	Tadschikistan
BE	Belgien	GN	Guinea	MK	Die ehemalige jugoslawische Republik Mazedonien	TM	Turkmenistan
BF	Burkina Faso	GR	Griechenland			TR	Türkei
BG	Bulgarien	HU	Ungarn	ML	Mali	TT	Trinidad und Tobago
BJ	Benin	IE	Irland	MN	Mongolei	UA	Ukraine
BR	Brasilien	IL	Israel	MR	Mauretanien	UG	Uganda
BY	Belarus	IS	Island	MW	Malawi	US	Vereinigte Staaten von Amerika
CA	Kanada	IT	Italien	MX	Mexiko		
CF	Zentralafrikanische Republik	JP	Japan	NE	Niger	UZ	Usbekistan
CG	Kongo	KE	Kenia	NL	Niederlande	VN	Vietnam
CH	Schweiz	KG	Kirgisistan	NO	Norwegen	YU	Jugoslawien
CI	Côte d'Ivoire	KP	Demokratische Volksrepublik Korea	NZ	Neuseeland	ZW	Zimbabwe
CM	Kamerun			PL	Polen		
CN	China	KR	Republik Korea	PT	Portugal		
CU	Kuba	KZ	Kasachstan	RO	Rumänien		
CZ	Tschechische Republik	LC	St. Lucia	RU	Russische Föderation		
DE	Deutschland	LI	Liechtenstein	SD	Sudan		
DK	Dänemark	LK	Sri Lanka	SE	Schweden		
EE	Estland	LR	Liberia	SG	Singapur		



## Einrichtung zur Diebstahlsicherung

Die Erfindung betrifft eine Einrichtung zur Diebstahlsicherung eines Kraftfahrzeuges mit einer Vorrichtung zur Deaktivierung des Fahrzeuges und einer Diebstahl-Detektionsvorrichtung, über welche eine unautorisierte Inbetriebnahme des Kraftfahrzeuges feststellbar und die Deaktivierungsvorrichtung betätigbar ist.

Bekannte Kraftfahrzeugs-Diebstahlsicherungen der vorgenannten Art melden den Versuch, in das Kraftfahrzeug einzudringen, es abzuschleppen, es zu heben oder an dieses anzustoßen mittels Alarmsignalen, die aus Ton- und/oder Lichtsignalen gebildet werden. Diese Anlagen bieten jedoch nur beschränkten Schutz, da die in der Umgebung lebende Bevölkerung besonders im dicht verbauten städtischen Bereich durch die große Anzahl an ständig auftretenden Fehlalarmen relativ passiv ist, wenn es darum geht, den ausgelösten Alarm der Exekutive zu melden.

Ein weiterer Lösungsweg besteht darin, verschiedene Kodierungs-Einheiten oder schwer zugängliche Sperrelemente an wichtigen Stellen im Auto vorzusehen, wodurch sich die aufgewendete Zeit für den erfolgreichen Diebstahl eines Kraftfahrzeugs erhöht und vom Autodieb zusätzlich eine relativ hohe Qualifikation erfordert. Der Nachteil dieser Diebstahlsicherungen besteht darin, daß erfahrungsgemäß auch sehr komplizierte technische Vorrichtungen bei ausreichend vorhandener Zeit überwunden werden können. Sollte aber ein Diebstahl an einer solchen unbezwingbaren Sicherung scheitern, äußert sich die Frustration darüber oftmals in einer schwerwiegenden Beschädigung des betreffenden Wagens oder der Inneneinrichtung desselben.

Eine weitere bekannte Möglichkeit der Diebstahlsicherung besteht darin, den Einbruch- bzw. Diebstahlversuch in das Auto nicht durch hör- oder sichtbare Alarmzeichen der Umgebung anzuzeigen, sondern diesen über einen eingebauten Sender an eine Empfangsstelle weiterzumelden, sodaß in weiterer Folge automatisch Sicherheitskräfte verständigt werden, die über Funkortung zum Ort des Geschehens kommen. Diese Dienstleistung kann aber nur in begrenzten Gebieten angeboten werden, weil einerseits keine flächendeckende Funkverbindung möglich ist und andererseits die Benachrichtigung eines Sicherheitsdienstes nur lokal vereinbart werden kann. Auch kann die Verfolgung eines mit dem gestohlenen Kraftfahrzeug fliehenden Autodiebs erhebliche Anstrengungen erfordern und darüber hinaus eine Beschädigung des gestohlenen Objekts zur Folge haben, wobei die

daraus entstehenden Kosten möglicherweise nicht durch eine Versicherung gedeckt sein können.

Aufgabe der Erfindung ist es daher, eine Vorrichtung zur Diebstahlsicherung anzugeben, mit welcher der Diebstahl eines Kraftfahrzeugs wirkungsvoll verhindert werden kann, ohne daß dem Autodieb Zeit gelassen wird, die getroffenen Sicherungsmaßnahmen ungestört und in Ruhe zu beseitigen.

Weitere Aufgabe der Erfindung ist es, Beschädigungen des gestohlenen Kraftfahrzeuges zu verhindern.

Weitere Aufgabe ist es, eine Sicherung gegen Diebstahl zu ermöglichen, bei welcher unter Wahrung der Sicherheit des Kraftfahrzeuglenkers die Auslösung einer Deaktivierung des Fahrzeugs selbsttätig erfolgt.

Erfindungsgemäß wird dies dadurch erreicht, daß die Deaktivierungsvorrichtung mit einer diese steuernden Zeitverzögerungseinheit verbunden ist, welche die Deaktivierung des Fahrzeugs erst nach Ablauf einer vorbestimmbaren Zeitspanne ab dem Zeitpunkt der unautorisierten Inbetriebnahme auslöst.

Auf diese Weise kann der Autodieb zwar den gestohlenen Wagen in Bewegung setzen und damit wegfahren, sobald er aber eine bestimmte Entfernung zurückgelegt hat, wird eine Unterbrechung einer für die Aufrechterhaltung des Fahrbetriebes notwendigen Funktion, z.B. der Benzinzufuhr, des Zündstromes usw., vorgenommen, wodurch das gerade in Fahrt befindliche Kraftfahrzeug zum Stehen gebracht wird und der Dieb sich nunmehr bereits auf einer dicht befahrenen Straße befindet, sodaß er zusätzlich zum Überraschungseffekt auch die Aufmerksamkeit der anderen Verkehrsteilnehmer auf sich zieht. Da für den Dieb nun keine Zeit zur Suche nach der Ursache des Stillstandes oder nach einer an irgend einer Stelle innerhalb des Kraftfahrzeugs angebrachten Unterbrechungseinrichtung verbleibt, ist er gezwungen, den gestohlenen Wagen zurückzulassen und die Flucht zu ergreifen.

In weiterer Ausbildung der Erfindung kann die Deaktivierungsvorrichtung - in an sich bekannter Weise - durch eine Einheit zur Unterbrechung der Benzinzufuhr oder des Zündstromes gebildet sein. Dadurch kann die Deaktivierung des Kraftfahrzeuges sehr rasch und wirkungsvoll vorgenommen werden, sodaß eine Fortsetzung der Fahrt mit dem gestohlenen Kraftfahrzeug nicht mehr möglich ist. Diese Deaktivierungsvorrichtungen können in erprobter Weise relativ klein ausgeführt werden, sodaß sie völlig unauffällig an

den geeigneten Stellen im Wageninneren für die Beendigung der Fahrt mit dem gestohlenen Fahrzeug sorgen.

Weiters kann gemäß einem weiteren Merkmal der Erfindung vorgesehen sein, daß die vorbestimmbare Zeitspanne in einem Bereich zwischen 20 Sekunden und 50 Sekunden liegt. Damit ist sichergestellt, daß der Autodieb sich in ausreichender Entfernung vom Ort des Diebstahls befindet, wenn das Kraftfahrzeug plötzlich nicht mehr weiterfährt. Die Gefahr einer weiteren Manipulation des Kraftfahrzeuges ist deutlich herabgesetzt, da der Autodieb nun nicht mehr damit rechnen kann, sein Werk in ungestörter Weise fortzusetzen. Damit ist das gestohlene Kraftfahrzeug auch weitgehend gegen mutwillige Zerstörungshandlungen geschützt, die sich aus dem mißglückten Diebstahlsversuch ergeben könnten.

Gemäß einer weiteren Variante der Erfindung kann die Diebstahl-Detektionsvorrichtung aus einer innerhalb des Kraftfahrzeugs angeordneten Empfangseinheit und einer tragbaren Sendeeinheit gebildet und eine Vorrichtung zur Überwachung der von der Sendeeinheit an die Empfangseinheit laufend gesendeten Sendesignale vorgesehen sein, sodaß die unautorisierte Inbetriebnahme des Fahrzeuges bei Verlassen des Sendebereiches der tragbaren Sendeeinheit detektiert und die Zeitverzögerungs-Einheit in Gang gesetzt wird, welche nach Ablauf der vorbestimmbaren Zeitspanne über die Deaktivierungsvorrichtung die Deaktivierung des Fahrzeuges automatisch auslöst.

Damit kann die Auslösung der erfindungsgemäßen Diebstahlsicherungseinrichtung vom aktuellen Aufenthaltsort des rechtmäßigen Besitzers abhängig gemacht werden. Setzt sich dieser mit der Sendeeinheit in das Kraftfahrzeug, so können mit diesem beliebige Distanzen zurückgelegt werden, ohne daß es dabei zu einem Verlassen des Sendebereiches kommen kann. Folglich wird auch kein Alarm ausgelöst, der eine spätere Deaktivierung des Kraftfahrzeuges zur Folge hätte. Sobald der Autobesitzer aber sein Fahrzeug verläßt, darf er sich nur innerhalb des Sendebereiches zu Fuß fortbewegen, ohne daß es zur Alarmauslösung kommt. Da er dies weiß, wird er sich immer in der richtigen Distanz vom Kraftfahrzeug aufhalten. Wird hingegen sein Auto aufgrund eines Diebstahls aus dem Sendebereich hinausbewegt, so kommt es nach Ablauf der vorbestimmbaren Zeitspanne zur Deaktivierung, wodurch das Fahrzeug wirkungsvoll gegen Diebstahl geschützt ist. Es kann das unerlaubte Inbetriebnehmen des Kraftfahrzeuges auch auf andere Weise festgestellt und dann erst die Deaktivierung des Kraftfahrzeuges eingeleitet werden.

Die Kombination aus Sende- und Empfangseinheit hat sich in der Praxis als sehr effizient herausgestellt.

Um die Gefahr eines Verkehrsunfalles herabzusetzen, kann gemäß weiterer Ausbildung der Erfindung vorgesehen sein, daß innerhalb des Kraftfahrzeugs eine Signalisierungseinheit vorgesehen ist, welche eine bestimmte Zeitspanne vor Auslösen der Deaktivierungsvorrichtung eine Anzeige- und/oder Wiedergabeeinheit aktiviert.

Damit kann der Autodieb mittels Lautsprecher oder Laufschriftanzeige rechtzeitig davon in Kenntnis gesetzt werden, daß das Kraftfahrzeug in der nächsten Zeit automatisch seinen Fahrbetrieb einstellen wird, wobei auch ein gewöhnliches Versagen des Motors oder anderer Teile des Kraftfahrzeuges vorgetäuscht werden kann, sodaß der Autodieb nicht erkennen kann, daß die Deaktivierung durch seine unautorisierte Inbetriebnahme ausgelöst worden ist.

Weiters betrifft die Erfindung ein Verfahren zur Diebstahlsicherung eines Kraftfahrzeuges, wobei eine unautorisierte Inbetriebnahme detektiert und das Fahrzeug deaktiviert wird, sodaß dieses fahruntauglich wird.

Aufgabe der Erfindung ist es, ein Verfahren der vorstehend genannten Art anzugeben, mit dem der Diebstahl auf eine für den Autodieb überraschende und unvorhersehbare Art verhindert wird.

Dies wird erfindungsgemäß dadurch erreicht, daß die Deaktivierung des Fahrzeugs erst nach einer vorbestimmbaren Zeitspanne ab der Detektion der unautorisierten Inbetriebnahme vorgenommen wird.

Auf diese Weise wähnt sich der Autodieb nach dem erfolgreichen Aufbrechen und Ingangsetzen des Fahrzeugs soweit in Sicherheit, daß er die Fahrt mit dem gestohlenen Fahrzeug aufnimmt und sich vom Ort des Diebstahl wegbewegt. Damit gelangt er mit hoher Wahrscheinlichkeit in belebtere Gegenden bzw. auf eine höher frequentierte Straße. Der Überraschungseffekt der Deaktivierung des Fahrzeugs tritt somit erst während der Fahrt und möglicherweise in Gegenwart von vielen anderen Verkehrsteilnehmern auf. Da der Autodieb darauf unvorbereitet ist, wird er versuchen, das zum Stillstand gekommene Fahrzeug zu verlassen und zu flüchten. Die Art und Weise, wie die Zeitverzögerung zwischen der Detektion der unautorisierten Inbetriebnahme und der Deaktivierung des Kraftfahrzeuges erreicht wird, ist im Rahmen der Erfindung frei gestaltbar. Dies kann durch eine Zeitverzögerungseinheit oder durch andere Maßnahmen erreicht werden, z.B. indem der mit

dem Kraftfahrzeug zurückgelegte Weg gemessen wird und ab einer bestimmten Distanz vom Ort des Diebstahls die Deaktivierung des Kraftfahrzeuges vorgenommen wird.

Eine andere Variante der Erfindung kann darin bestehen, daß über eine Sendeeinheit an eine im Kraftfahrzeug angeordnete Empfangseinheit laufend Sendesignale gesendet werden, und daß die unautorisierte Inbetriebnahme detektiert wird, sobald von der Empfangseinheit keine Sendesignale der Sendeeinheit empfangen werden, und daß darauffolgend nach Ablauf der vorbestimmbaren Zeitspanne die Deaktivierung des Kraftfahrzeuges vorgenommen wird.

Sobald der Autodieb den Sendebereich verläßt, wird der Verlust des Autos festgestellt. Dies soll nur weit genug vom Besitzer entfernt geschehen, damit der Dieb nicht mehr gewalttätig gegenüber diesem werden kann. Ob dabei die Sendereichweite aufgrund der atmosphärischen Bedingungen einer Streuung unterliegt, ist unerheblich. Die automatische Abstellung des Fahrtbetriebs hat gegenüber bekannten Lösungen den großen Vorteil, daß der Autofahrer nicht ständig darauf achten muß, ob sein Fahrzeug gestohlen wird. Sollte ihm das Auto auf offener Straße geraubt und er dabei bewußtlos geschlagen werden, erlaubt die erfindungsgemäße Sendebereichsdetektion eine Auslösung der Fahrzeugsperre ohne aktive Mitwirkung des Fahrers, wohingegen bei bekannten Sicherheitssystemen der Fahrzeugbesitzer bei Bewußtsein sein und das Fahrzeug ständig unter Beaufsichtigung haben muß.

In weiterer Ausbildung der Erfindung kann unmittelbar vor der Deaktivierung des Kraftfahrzeugs im Inneren desselben eine Anzeige- und/oder Wiedergabeeinheit aktiviert werden, über die dem Fahrer des Kraftfahrzeugs mitgeteilt wird, daß es zu einer Fahrtunterbrechung des Kraftfahrzeuges kommen wird.

Damit sollen gefährliche Verkehrssituationen, die sich infolge der plötzlichen Fahrtunterbrechung ergeben könnten, vermieden werden.

Nachfolgend wird die Erfindung anhand der in den Zeichnungen dargestellten Ausführungsbeispiele eingehend erläutert. Es zeigt dabei

Fig.1 ein Blockschaltbild einer Ausführungsform der erfindungsgemäßen Einrichtung zur Diebstahlsicherung ohne Deaktivierungsvorrichtung;

Fig.2 ein Schema des logischen Ablaufs des erfindungsgemäßen Verfahrens;

Fig.3 ein Blockschaltbild einer Ausgestaltung der Empfangseinheit gemäß

Fig.1 und

Fig.4 ein Blockschaltbild einer Ausgestaltung der Sendeeinheit gemäß Fig.1.

Das in Fig.1 dargestellte Blockschaltbild zeigt eine Diebstahl-Detektionsvorrichtung 1, 2, welche Teil einer Einrichtung zur Diebstahlsicherung eines Kraftfahrzeuges ist und über welche eine unautorisierte Inbetriebnahme des Kraftfahrzeuges feststellbar ist. Die Einrichtung zur Diebstahlsicherung 1,2 umfaßt weiters eine nicht dargestellte Vorrichtung zur Deaktivierung des Fahrzeuges, welche über die Diebstahl-Detektionsvorrichtung 1,2 betätigt wird, sobald eine unautorisierte Inbetriebnahme detektiert wird. Unter Kraftfahrzeug wird dabei jede Art von motorgetriebenem Fahrzeug verstanden, z.B. ein Personenkraftwagen, ein Lastwagen, ein Motorrad usw..

Erfindungsgemäß ist vorgesehen, daß die Deaktivierungsvorrichtung mit einer diese steuernden Zeitverzögerungseinheit verbunden ist, welche die Deaktivierung des Fahrzeugs erst nach Ablauf einer vorbestimmbaren Zeitspanne ab dem Zeitpunkt der unautorisierten Inbetriebnahme auslöst. Mit Hilfe der in Fig.1 nicht gesondert dargestellten Zeitverzögerungseinheit soll im wesentlichen die durch die Diebstahl-Detektionsvorrichtung 1, 2 betätigte Deaktivierungsvorrichtung nicht sofort sondern erst nach der vorbestimmbaren Zeitspanne wirksam werden.

Die Diebstahl-Detektionsvorrichtung ist gemäß Fig.1 bevorzugt aus einer im Kraftfahrzeug angeordneten Empfangseinheit 1 und einer tragbaren, im Normalbetrieb innerhalb eines durch den Sendebereich bestimmten, maximalen Abstandes befindlichen Sendeeinheit 2 gebildet, wobei die unautorisierte Inbetriebnahme des Fahrzeuges bei Verlassen des Sendebereiches detektiert wird.

Der innerhalb der Empfangseinheit 1 angeordnete Empfangsteil 11 erhält sein Eingangssignal von einer Empfangsantenne 4 und wandelt dieses in ein geeignetes weiterverarbeitbares Signal um. Zur Ausschaltung von unerwünschten Beeinflussungen durch andere Sender ist das von der Sendeeinheit 2 gesendete Signal vorzugsweise kodiert und wird daher in einer Dekodiereinheit 12 dekodiert und an den einen Eingang einer Bearbeitungseinheit 15 weitergeleitet, deren Ausgang mit einer Auslöseeinheit 16 verbunden ist, über welche die Deaktivierungsvorrichtung aktiviert wird. Der zweite Eingang der Bearbeitungseinheit 15 ist mit einer Sensoreinheit 13 verbunden, die über nicht dargestellte Sensoren eine Vergleichsmessung vornimmt und das Meßsignal der Bearbeitungseinheit zur Verfügung stellt. Die Sensoreinheit 13 überwacht etwa das Vorhandensein einer Aktivität des Motors vom zu schützenden Kraftfahrzeug oder die Drehbewegung der Fahrzeugräder.

Der Ausgang der Auslöseeinheit 16 ist durch eine Schnittstelle 5 gebildet, über die der Datenverkehr mit der Deaktivierungsvorrichtung abläuft.

Die Deaktivierung des Fahrzeugs kann auf verschiedene Weise erfolgen, in der überwiegenden Anzahl der möglichen Fälle wird dabei eine Hauptfunktion des Motors ausgeschaltet werden, so kann etwa die Benzinzufuhr über ein Zufuhrmagnetventil oder durch Beeinflussung der Benzinpumpe sowie der Zündstromkreis mittels geeigneter Einheiten unterbrochen werden, wodurch der Antrieb des Kraftfahrzeuges gesperrt wird und ein Weiterfahren verunmöglicht wird. Im Unterschied zu anderen, bekannten Diebstahlsicherungseinrichtungen wird die Deaktivierung aber nicht am Ort des Diebstahls vorgenommen, sondern erst nach einer bestimmten Zeitspanne, in der der Dieb mit großer Wahrscheinlichkeit bereits auf einem höher frequentierten Verkehrsweg unterwegs ist. Da er mit einem Ausfall des Kraftfahrzeuges auf offener Straße nicht rechnet, wird der Dieb in den meisten Fällen nicht versuchen, die Ursache des plötzlichen Ausfalls zu suchen sondern möglichst schnell die Flucht ergreifen, um nicht weiter die Aufmerksamkeit der anderen Verkehrsteilnehmer auf sich zu ziehen, da die Gefahr einer Polizeikontrolle in dieser Situation doch deutlich erhöht ist.

Um nun die Gefahr eines Verkehrsunfalls zu vermindern ist innerhalb des Kraftfahrzeuges eine Signalisierungseinheit 17 vorgesehen ist, welche eine bestimmte Zeitspanne vor Auslösen der Deaktivierungsvorrichtung eine Anzeige- und/oder Wiedergabeeinheit aktiviert. In Fig.1 ist dafür ein Lautsprecher 3 vorgesehen, der eine warnende Mitteilung an den das Kraftfahrzeug lenkenden Autodieb weitergibt. Dies kann in beliebiger Weise mittels Tonband oder Sprachprozessor vorgenommen werden.

Die Durchsage kann etwa aus den folgenden Sätzen bestehen: " ACHTUNG STILLSTAND DES FAHRZEUGES TRITT IN EINER MINUTE EIN, BITTE FAHREN SIE AN DEN STRASSENRAND." Da der Dieb nicht ahnen kann, daß diese Fahrtunterbrechung durch seine Aktivitäten ausgelöst worden ist, wird er annehmen, daß es sich um eine Automatik des Fahrzeuges handelt und tatsächlich das Fahrzeug zur Seite chauffieren.

Fig.2 zeigt ein typisches Ablaufdiagramm für die Ausführung des erfindungsgemäßen Verfahrens zur Diebstahlsicherung eines Kraftfahrzeuges, welches darin besteht, daß die Deaktivierung des Fahrzeugs erst nach einer vorbestimmbaren Zeitspanne ab der Detektion der unautorisierten Inbetriebnahme vorgenommen wird. Unmittelbar vor der

Deaktivierung des Fahrzeugs im Inneren desselben wird eine Anzeige- und/oder Wiedergabeeinheit aktiviert, über die dem Fahrer des Kraftfahrzeugs mitgeteilt wird, daß es zu einer Fahrtunterbrechung des Kraftfahrzeuges kommen wird.

Fig.3 zeigt eine konkrete Ausgestaltung einer Schaltungsanordnung, mit der eine Empfangseinheit und eine Deaktivierungsvorrichtung verwirklicht werden kann.

Der Empfangsteil 11 ist an seinem Eingang mit der Antenne 4 verbunden, welche die Signale der Sendeeinheit 2 empfängt und demoduliert. Am Ausgang ist der Empfangsteil 11 an den Eingang eines Verstärkers 31 geschaltet, der das empfangene Signal verstärkt und an einen Eingang des Mikroprozessors 32 weitergibt. Ein weiterer Eingang des Mikroprozessors 32 ist mit dem Ausgang der Sensoreinheit 13 verbunden, die eine für den Betrieb des Fahrzeuges charakteristische Funktion, z.B. die Zündspannung oder die Ausgangsspannung der Lichtmaschine, mißt und den gemessenen Wert an den Mikroprozessor weitergibt. Genauso könnte die Umdrehungszahl eines der vier Räder des Kraftfahrzeuges mittels eines geeigneten Sensors gemessen werden, um den Betrieb des Kraftfahrzeuges verläßlich nachzuweisen.

Im Mikroprozessor 32, welcher eine zentrale Steuer- und Recheneinheit ausbildet, werden die an den dessen Eingängen anliegenden Signale gewandelt und weiterverarbeitet und dementsprechend Ausgänge A2, A3 und A4 gesteuert. Die Ausgänge A2 und A3 sind mit Einheiten 34, 35 verbunden, über die verschiedene Stromkreise 36, 37 unterbrochen werden können. Diese können z.B. der Versorgungsstromkreis für die Benzinpumpe oder der Zündstromkreis sein. Damit kann die Benzinzufuhr und der Zündstromkreis unterbrochen werden. Somit bilden die Einheiten 34, 35 die in Fig.1 nicht dargestellte Deaktivierungsvorrichtung. Diese kann wie bereits vorstehend erwähnt sehr vielfältig auf die Wirkungsweise des Fahrzeuges einwirken. Ihre Hauptfunktion besteht darin, den Fahrbetrieb des Kraftfahrzeuges an einer möglichst unzugänglichen Stelle innerhalb des Fahrzeuges zu unterbrechen.

Gemäß der Erfindung soll die Deaktivierung des Kraftfahrzeuges erst nach einer vorbestimmbaren Zeitspanne erfolgen. Die Berechnung bzw. Überwachung dieser Zeitspanne geschieht über den Mikroprozessor 32, der nach Detektion des Diebstahls den Befehl zur Deaktivierung des Fahrzeuges erst nach der eingebbaren Zeitspanne an die Einheiten 34, 35 weitergibt. Damit geschieht die automatische Fahrtunterbrechung erst nachdem der Dieb sich bereits ins Auto gesetzt hat und mit diesem davon gefahren ist.



An Ausgang A4 des Mikroprozessors 32 ist die Wiedergabe-Einheit 17 angeschlossen, die z.B. durch einen Sprachprozessor gebildet sein kann, und über die mittels des in der Fahrgastzelle angebrachten Lautsprechers 3 eine Durchsage an den Fahrer übermittelt werden kann, die je nach Land und Sprachen anders lauten kann. Anstelle oder in Kombination dazu kann auch eine entsprechende optische Wiedergabeeinheit vorgesehen sein, auf der eine Warnung angezeigt werden kann, in welcher Weise und ab welchem Zeitpunkt mit einer Fahrtunterbrechung zu rechnen sein wird.

Im wesentlichen soll über die Wiedergabe-Einheit 17 der sich auf der Flucht befindliche Dieb kurz vor Deaktivierung des Fahrzeuges, also vor dem nahenden Stillstand des Fahrzeuges gewarnt werden, um nicht eine unnötige Unfallsgefahr zu provozieren.

Fig.4 zeigt ein Blockschaltbild mit einer konkreten Realisierung der Sendeeinheit 2 der Diebstahl-Detektionsvorrichtung, die immer in der Nähe des Kraftfahrzeug-Inhabers aufbewahrt und vorzugsweise nicht an seinem Autoschlüssel befestigt werden sollte.

Ein Mikroprozessor 42 enthält jene Kodierungsvorschrift, die mit dem in der Empfangseinheit 1 gespeicherten Kode übereinstimmt. Über einen Schalter 41 kann der Betrieb der Sende-Einheit 2 ein- und ausgeschaltet werden. Der Mikroprozessor 42 erzeugt ein kodierte Signal, das über den Sendeteil 22 und über eine Antenne 44 ständig gesendet wird. Das so abgesandte Sendesignal wird von der Empfangseinheit 1 empfangen, solange diese sich innerhalb der Sendereichweite des Senders 22 befindet. Wenn das empfangene Signal nach Dekodierung den vorgegebenen Werten entspricht, wird dies als Normalbetrieb gewertet, während dem keine Deaktivierung des Fahrzeuges vorgenommen werden soll. Eine Leuchtdiode 43 ist dabei zusätzlich vorgesehen, damit der Fahrzeugbesitzer sich vom dauernden Sendebetrieb und somit von der Funktionsfähigkeit seiner Diebstahlsicherungseinrichtung überzeugen kann.

Dies entspricht der realen Situation, in der der Besitzer des Fahrzeuges sein Fahrzeug irgendwo abstellt und sich zu einem nahegelegenen Ort zu Fuß begibt, z.B. an seinen Arbeitsplatz, in seine Wohnung oder auf Besuch bei Bekannten. Er schließt das Fahrzeug ab und nimmt zugleich die Sendeeinheit 2 mit sich, während die Empfangseinheit im Fahrzeug an einer verborgenen Stelle zurückbleibt. Dabei ist der Sendebereich so abgestimmt, daß dieser eine nähere Umgebung, z.B. eine maximale Entfernung von 300m, abdeckt. Die Sendeeinheit 2 sendet laufend ihr Sendesignal und die Empfangseinheit 1

empfängt dieses laufend und wandelt es nach der Dekodierungsvorschrift im Fahrzeug um. Der Mikroprozessor 32 (Fig.3) wertet diesen Zustand als Normalbetriebszustand, in dem über die Aktivierungseinheiten 36, 37 keine Maßnahmen zur Betriebsunterbrechung des Kraftfahrzeuges getroffen werden. Zusätzlich wird der Motorbetriebszustand über die Sensor-Einheit 13 ständig überwacht und die daraus gewonnene Information mitverarbeitet.

Befindet sich das Fahrzeug somit in Bewegung, es treffen aber dennoch ständig richtig kodierte Signale in der Empfangseinheit 1 ein, so bedeutet dies, daß sich der autorisierte Benutzer des Fahrzeuges mit der Sendeempfangseinheit 2 im Kraftfahrzeug befindet und daher eine beliebige Ortsveränderung möglich ist, ohne daß es zu einem Verlassen des Sendebereiches kommen könnte.

Tritt nun der Fall eines Autodiebstahls ein, bei dem der Autobesitzer sein Auto versperrt und sich zu einem nahegelegenen Ort begeben hat, so wird es dem Dieb nach einigen Versuchen gelingen, in das Kraftfahrzeug einzudringen und dort die üblichen Sicherungen gegen eine unautorisierte Inbetriebnahme überwinden. So wird er z.B. die Zündungskabel im Bereich der Lenkradsäule auftrennen und miteinander verbinden und so das Zündschloß überbrücken. Setzt er sich nun in Bewegung und verläßt den Ort des Geschehens, so wird er versuchen möglichst schnell aus der Gegend, in der er den Diebstahl verübt hat, zu verlassen. Dabei gelangt er aber unweigerlich auch außerhalb des Sendebereiches, wodurch die Empfangseinheit 1 keine kodierte Sendesignale des an seinem Aufenthaltsort verweilenden Fahrzeugbesitzers mit der Sendeeinheit 2 empfangen kann. Sobald keine Sendesignale mehr empfangen werden, bewertet dies der Mikroprozessor 32, der eine Vorrichtung zur Überwachung der von der Sendeeinheit 2 an die Empfangseinheit 1 laufend gesendeten Sendesignale bildet, als Alarmzustand. Damit wird die unautorisierte Inbetriebnahme des Fahrzeuges bei Verlassen des Sendebereiches der tragbaren Sendeeinheit 2 detektiert.

Ab diesem Zeitpunkt wird nun über eine im Mikroprozessor 32 beinhaltete bzw. durch diesen verwirklichte Zeitverzögerungs-Einheit eine Zeitautomatik in Gang gesetzt.

Die Zeitspanne dafür ist vorbestimmbar und kann z.B. im Bereich zwischen 20 und 50 Sekunden liegen. Erst nach Ablauf dieser Zeitspanne wird die Deaktivierungsvorrichtung 34, 35 automatisch ausgelöst, welche einen Stillstand des

Kraftfahrzeuges zur Folge hat. Die Deaktivierungsvorrichtung 34, 35 kann wie bereits vorstehend beschrieben z.B. die Benzinpumpe oder den Zündstromkreis unterbrechen.

Der Alarmzustand kann zusätzlich von der Bedingung abhängig gemacht werden, ob die Sensoreinheit 13 einen Motorbetrieb feststellt oder nicht. Da das Kraftfahrzeug aber unter Umständen auch durch Abschleppen oder durch Huckepack-Verfrachtung gestohlen werden kann, ist das Kriterium des Wegfalls der empfangenen kodierte Signale das am sichersten zu verwertende.

Eine bestimmte Zeitspanne vor der Deaktivierung des Kraftfahrzeuges kann nun über die Wiedergabeeinheit 17 und den Lautsprecher 3 die Mitteilung an den Fahrer weitergegeben werden, daß er das Fahrzeug am Straßenrand zum Stillstand bringen sollte.

Als Verstärkung des Effekts kann das Fahrzeug bei der Deaktivierung zusätzlich über die Hup- und Schweinwerferanlage des Fahrzeuges visuelle und akustische Signale abgeben, um das gestohlene Auto möglichst auffällig zu machen. Der Dieb befindet sich in einer völlig unvorbereiteten Situation und wird daher möglichst schnell das Weite suchen.

Eine verschärfte Form des Autodiebstahls ist das sogenannte car-jacking, das einem Autoraub auf offener Straße entspricht. Dabei werden die Kraftfahrzeuglenker bei Anhalten des Fahrzeuges z.B. an einer Kreuzung gewalttätig zur Übergabe des Autos mit dem angesteckten Fahrzeugschlüssel gezwungen und der Räuber kann das Auto auf diese Weise ungehindert in seine Gewalt bringen. Hat der Kraftfahrzeug-Besitzer die Sendeeinheit nun nicht an seinem Autoschlüssel befestigt und nicht im Auto abgelegt, sondern trägt er diese in einer Kleidungstasche bei sich, so wird die erfindungsgemäße Diebstahlsautomatik ebenfalls in Gang gesetzt. Der Autodieb entfernt sich vom Besitzer des gestohlenen Kraftfahrzeugs und verläßt dabei den Sendebereich des Senders. Sobald dieser verlassen ist, wird die Zeitverzögerungseinheit aktiviert und die Deaktivierung des Fahrzeugs nach der vorbestimmbaren Zeitspanne automatisch vorgenommen. Dies hat den entscheidenden Vorteil, daß der Autodieb sich bereits außerhalb der Reichweite des rechtmäßigen Kraftfahrzeugbesitzers befindet, wenn die Unterbrechung des Fahrbetriebs auftritt. Dadurch kann der Dieb bzw. der Räuber diesen nicht zwingen, die Deaktivierungseinheit aufzuheben und muß das gestohlene Kraftfahrzeug unverrichteter Dinge zurücklassen.

Nachfolgend ist ein Beispiel für den Zeitablauf innerhalb einer Empfangs- und einer Sendeeinheit beschrieben.

Die Empfangseinheit 1 verbleibt im Normalbetriebszustand solange diese eine von der Sendeeinheit 2 gesendete, kodierte Signalreihe erkennt. Dazu muß sich der Fahrzeugbesitzer in der näheren Umgebung vom Fahrzeug befinden. Nach Empfangen einer störungsfrei eingetroffenen Signalreihe bleibt die Sendeeinheit für 120 Sekunden im deaktivierten Zustand. Falls die Signalreihen nicht mehr empfangen werden, weil das Fahrzeug sich vom Besitzer entfernt hat, wird die Deaktivierungsvorrichtung nach Ablauf der Verzögerungszeit aktiviert. Diese kann z.B. 30 Sekunden betragen. Bevor dies geschieht, kann über den Lautsprecher 3 der Warntext wiedergegeben werden. Als zusätzliche Maßnahmen kann nun auch für die anderen Verkehrsteilnehmer erkennbar die Warnblinkanlage und gegebenenfalls die Hupe intermittierend eingeschaltet werden. Nach Ende der Warnmitteilung geht die Empfangseinheit in den Alarmbetrieb über, indem die Deaktivierungsvorrichtung automatisch betätigt wird.

Die Sendeeinheit kann folgendermaßen konzipiert sein:

Wiederholzeit der Sendungen:	20 Sekunden
Sendezeit:	150 ms
Trägerfrequenz:	433, 92 MHz
Frequenzabweichung:	+/- 100 kHz
Ausgestrahlte Leistung:	100 mW

## PATENTANSPRÜCHE

1. Einrichtung zur Diebstahlsicherung eines Kraftfahrzeuges mit einer Vorrichtung zur Deaktivierung des Fahrzeuges (34, 35) und einer Diebstahl-Detektionsvorrichtung (1, 2), über welche eine unautorisierte Inbetriebnahme des Kraftfahrzeuges feststellbar und die Deaktivierungsvorrichtung (34, 35) betätigbar ist, **dadurch gekennzeichnet**, daß die Deaktivierungsvorrichtung (34, 35) mit einer diese steuernden Zeitverzögerungseinheit verbunden ist, welche die Deaktivierung des Fahrzeugs erst nach Ablauf einer vorbestimmbaren Zeitspanne ab dem Zeitpunkt der unautorisierten Inbetriebnahme auslöst.
2. Einrichtung nach Anspruch 1, **dadurch gekennzeichnet**, daß die Deaktivierungsvorrichtung (34, 35) - in an sich bekannter Weise - durch eine Einheit zur Unterbrechung der Benzinzufuhr oder des Zündstromes gebildet ist.
3. Einrichtung nach Anspruch 1 oder 2, **dadurch gekennzeichnet**, daß die vorbestimmbare Zeitspanne in einem Bereich zwischen 20 und 50 Sekunden liegt.
4. Einrichtung nach Anspruch 1, 2 oder 3, **dadurch gekennzeichnet**, daß die Diebstahl-Detektionsvorrichtung aus einer innerhalb des Kraftfahrzeugs angeordneten Empfangseinheit (1) und einer tragbaren Sendeeinheit (2) gebildet ist, und daß eine Vorrichtung zur Überwachung der von der Sendeeinheit (2) an die Empfangseinheit (1) laufend gesendeten Sendesignale vorgesehen ist, sodaß die unautorisierte Inbetriebnahme des Fahrzeuges bei Verlassen des Sendebereiches der tragbaren Sendeeinheit (2) detektiert und die Zeitverzögerungs-Einheit in Gang gesetzt wird, welche nach Ablauf der vorbestimmbaren Zeitspanne über die Deaktivierungsvorrichtung (34, 35) die Deaktivierung des Fahrzeugs automatisch auslöst.
5. Einrichtung nach Anspruch 1 bis 4, **dadurch gekennzeichnet**, daß innerhalb des Kraftfahrzeuges eine Signalisierungseinheit (17) vorgesehen ist, welche eine bestimmte

Zeitspanne vor Auslösen der Deaktivierungsvorrichtung eine Anzeige- und/oder Wiedergabeeinheit (3) aktiviert.

6. Verfahren zur Diebstahlsicherung eines Kraftfahrzeuges, wobei eine unautorisierte Inbetriebnahme detektiert und das Fahrzeug deaktiviert wird, sodaß dieses fahruntauglich wird, **dadurch gekennzeichnet**, daß die Deaktivierung des Fahrzeugs erst nach einer vorbestimmbaren Zeitspanne ab der Detektion der unautorisierten Inbetriebnahme vorgenommen wird.

7. Verfahren nach Anspruch 6, **dadurch gekennzeichnet**, daß über eine Sendeeinheit (2) an eine im Kraftfahrzeug angeordnete Empfangseinheit (1) laufend Sendesignale gesendet werden, und daß die unautorisierte Inbetriebnahme detektiert wird, sobald von der Empfangseinheit (1) keine Sendesignale der Sendeeinheit (2) empfangen werden, und daß darauffolgend nach Ablauf der vorbestimmbaren Zeitspanne die Deaktivierung des Kraftfahrzeuges vorgenommen wird.

8. Verfahren nach Anspruch 6 oder 7, **dadurch gekennzeichnet**, daß unmittelbar vor der Deaktivierung des Fahrzeugs im Inneren desselben eine Anzeige- und/oder Wiedergabeeinheit (3) aktiviert wird, über die dem Fahrer des Kraftfahrzeuges mitgeteilt wird, daß es zu einer Fahrtunterbrechung des Kraftfahrzeuges kommen wird.

1/3

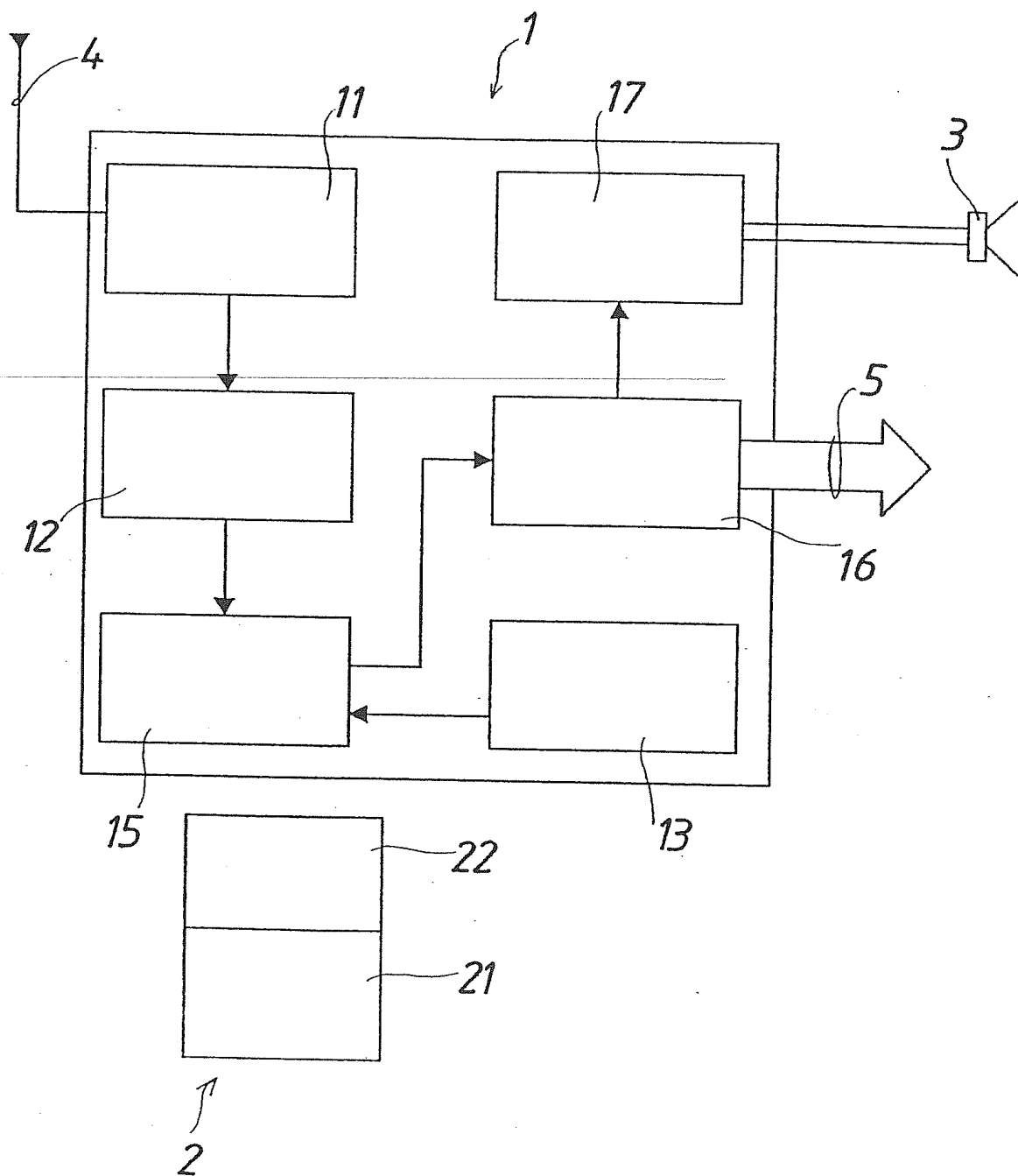
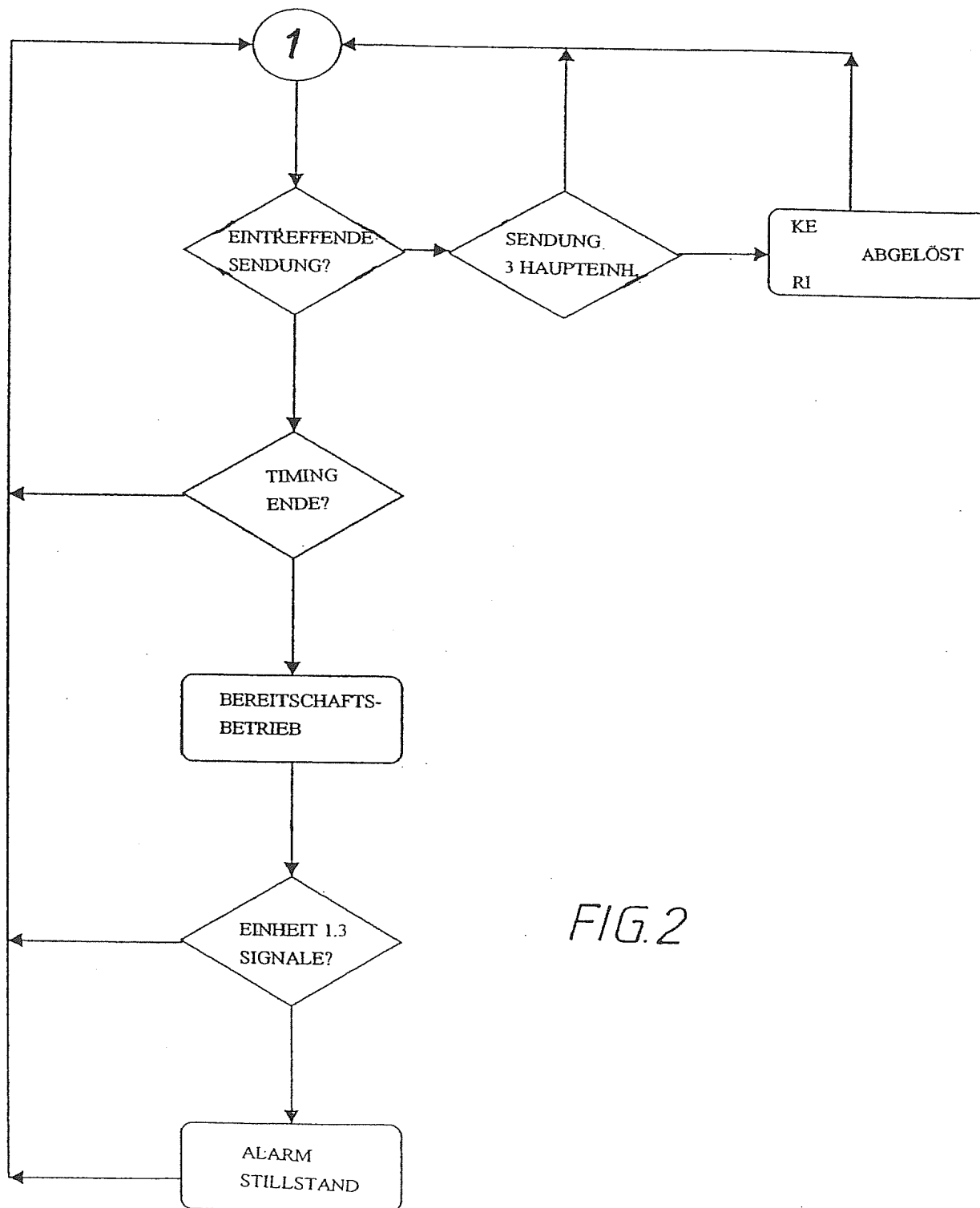


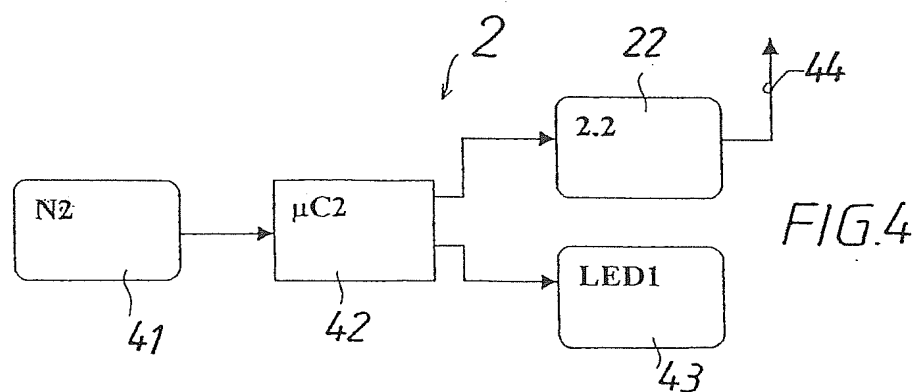
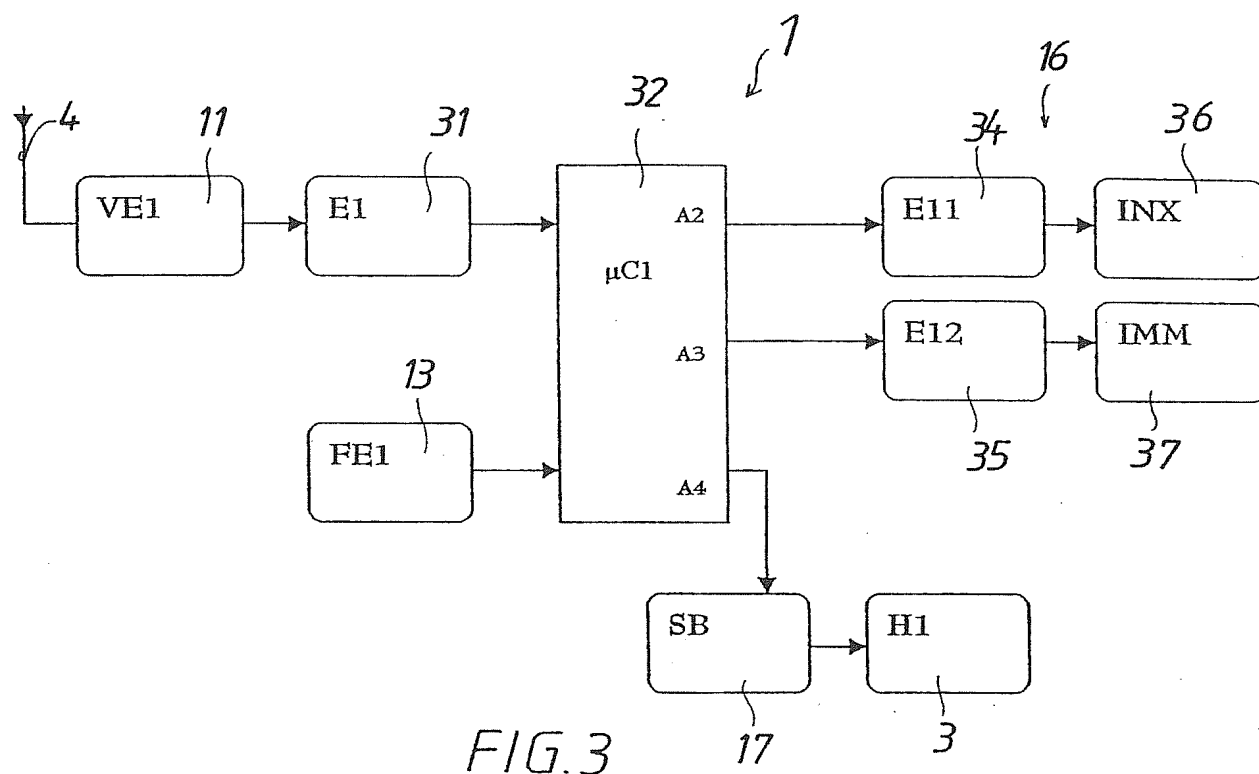
FIG.1

2/3





3/3



# INTERNATIONAL SEARCH REPORT

International Application No

PCT/AT 00/00031

**A. CLASSIFICATION OF SUBJECT MATTER**  
IPC 7 B60R25/04

According to International Patent Classification (IPC) or to both national classification and IPC

**B. FIELDS SEARCHED**

Minimum documentation searched (classification system followed by classification symbols)  
IPC 7 B60R E05B

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 0 641 693 A (DEPROMAX LTD) 8 March 1995 (1995-03-08) column 5, line 10 - column 6, line 22	1,2,5,6, 8
X A	US 5 559 491 A (STADLER DAVID M) 24 September 1996 (1996-09-24) column 3, line 15 - column 4, line 17 column 5, line 23 - line 37; figure 1	1-3,5,6, 8 4,7
X	US 5 793 306 A (VERSHININ MICHAEL ET AL) 11 August 1998 (1998-08-11) column 4, line 23 - line 34 column 7, line 25 - line 58	1-4,6,7
X	US 4 222 033 A (BROWN LEONARD L) 9 September 1980 (1980-09-09) column 3, line 19 - line 42	1-3,6

☐ Further documents are listed in the continuation of box C.



Patent family members are listed in annex.

\* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search

30 May 2000

Date of mailing of the international search report

07/06/2000

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2  
NL - 2280 HV Rijswijk  
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,  
Fax: (+31-70) 340-3016

Authorized officer

Eklom, H

# INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/AT 00/00031

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
EP 0641693	A	08-03-1995	US 5473200 A	05-12-1995
			AU 6892194 A	02-03-1995
			CN 2243414 U	25-12-1996
			ZA 9405777 A	14-03-1995
US 5559491	A	24-09-1996	US 5394135 A	28-02-1995
			US 5172094 A	15-12-1992
			WO 9311004 A	10-06-1993
US 5793306	A	11-08-1998	NONE	
US 4222033	A	09-09-1980	NONE	

**A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES**  
**IPK 7 B60R25/04**

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

**B. RECHERCHIERTE GEBIETE**

Recherchierte Mindestprüfstoff (Klassifikationssystem und Klassifikationsymbole)  
**IPK 7 B60R E05B**

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

**C. ALS WESENTLICH ANGESEHENE UNTERLAGEN**

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	EP 0 641 693 A (DEPROMAX LTD) 8. März 1995 (1995-03-08) Spalte 5, Zeile 10 - Spalte 6, Zeile 22	1, 2, 5, 6, 8
X A	US 5 559 491 A (STADLER DAVID M) 24. September 1996 (1996-09-24) Spalte 3, Zeile 15 - Spalte 4, Zeile 17 Spalte 5, Zeile 23 - Zeile 37; Abbildung 1	1-3, 5, 6, 8 4, 7
X	US 5 793 306 A (VERSHININ MICHAEL ET AL) 11. August 1998 (1998-08-11) Spalte 4, Zeile 23 - Zeile 34 Spalte 7, Zeile 25 - Zeile 58	1-4, 6, 7
X	US 4 222 033 A (BROWN LEONARD L) 9. September 1980 (1980-09-09) Spalte 3, Zeile 19 - Zeile 42	1-3, 6



Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen



Siehe Anhang Patentfamilie

\* Besondere Kategorien von angegebenen Veröffentlichungen :

"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist

"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist

"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)

"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht

"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist

"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist

"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden

"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist

"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche

30. Mai 2000

Absendedatum des internationalen Recherchenberichts

07/06/2000

Name und Postanschrift der Internationalen Recherchenbehörde  
 Europäisches Patentamt, P.B. 5818 Patentlaan 2  
 NL - 2280 HV Rijswijk  
 Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,  
 Fax: (+31-70) 340-3016

Bevollmächtigter Bediensteter

Eklom, H

# INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichung...; die zur selben Patentfamilie gehören

Intern: ~~als~~ Aktenzeichen

PCT/AT 00/00031

Im Recherchenbericht angeführtes Patentedokument		Datum der Veröffentlichung	Mitglied(er) der Patentfamilie		Datum der Veröffentlichung
EP 0641693	A	08-03-1995	US	5473200 A	05-12-1995
			AU	6892194 A	02-03-1995
			CN	2243414 U	25-12-1996
			ZA	9405777 A	14-03-1995
US 5559491	A	24-09-1996	US	5394135 A	28-02-1995
			US	5172094 A	15-12-1992
			WO	9311004 A	10-06-1993
US 5793306	A	11-08-1998	KEINE		
US 4222033	A	09-09-1980	KEINE		

Deutsches  
Patent- und Markenamt



DEPATISnet

Beginner

Expert

Ikofax

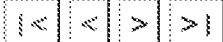
Family

Assistant



> DEPATISnet-Home > Search > Family > Result list > Bibliographic data

## Bibliographic data

**Document DE000019529666C1 (Pages: 6)**

Navigation in hitlist  (1 / 3)

BIBLIOGRAPHIC DATA DOCUMENT DE000019529666C1 (PAGES: 6)		
Criterion	Field	Contents
Title	TI	[DE] Verfahren zum Initialisieren eines Diebstahlschutzsystems für ein Kraftfahrzeug [EN] Initialisation procedure for vehicle anti-theft deterrent
Applicant	PA	Siemens AG, 80333 München, DE
Inventor	IN	Röhl, Thomas, 93092 Barbing, DE ; Sedlmeier, Martin, 93336 Altmannstein, DE ; Fest, Dieter, 93057 Regensburg, DE
Application date	AD	11.08.1995
Application number	AN	19529666
Country of application	AC	DE
Publication date	PUB	05.12.1996
Priority data	PRC PRN PRD	
IPC main class	ICM	<u>B60R 25/04</u>
IPC secondary class	ICS	
IPC additional class	ICA	
IPC index class	ICI	
MCD main class	MCM	
MCD secondary class	MCS	<u>B60R 25/04</u> (2006.01) A, , I, 20051008, R, M, EP
MCD additional class	MCA	
Abstract	AB	[ ] Für eine Wegfahrsperre mit mehreren tragbaren Transpondern T ↓ ↓ und einem Steuergerät 2 im Kraftfahrzeug sind eine vorbestimmte Anzahl von Freistarts erlaubt, ohne daß ein gültiges Codesignal empfangen werden muß. Sobald zwei Transponder T ↓ ↓ nacheinander das Steuergerät 2 aktivieren, wird das Diebstahlschutzsystem initialisiert. Freistarts sind dann nicht mehr möglich.

		<p>[EN]</p> <p>The procedure involves a system which includes several transportable transponders each comprising a store for storage of vehicle-specific data. A control device (2) is located in the vehicle. It requests a transponder to send data, during an activating procedure. It receives the data for comparison with specified or desired data, and is designed to enable functional tests to be carried out and all the associated transponders to initialised. Thus, with agreement of the compared data, a release signal is generated to allow starting of the vehicle. The release signal is automatically generated within a given number of activating events. All transponders in the anti-theft protection system have new data stored in them and new specified data is stored in the control device (2).</p>
Information on correction	KORRINF	
Cited documents	CT	<p><a href="#">DE00000431711A1</a> </p> <p><a href="#">DE000004333474A1</a> </p>
Cited non-patent literature	CTNP	

[Back to result list](#)[Report data error](#)[Print](#)[PDF display](#)



DEUTSCHES  
PATENTAMT

②1 Aktenzeichen: 195 29 666.4-51  
②2 Anmeldetag: 11. 8. 95  
④3 Offenlegungstag: —  
④5 Veröffentlichungstag  
der Patenterteilung: 5. 12. 96

Innerhalb von 3 Monaten nach Veröffentlichung der Erteilung kann Einspruch erhoben werden

⑦3 Patentinhaber:  
Siemens AG, 80333 München, DE

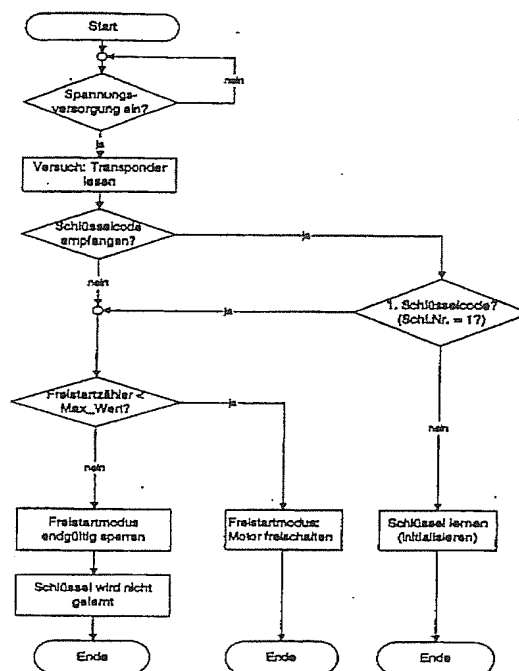
⑦2 Erfinder:  
Röhl, Thomas, 93092 Barbing, DE; Sedlmeier,  
Martin, 93336 Altmannstein, DE; Fest, Dieter, 93057  
Regensburg, DE

⑤6 Für die Beurteilung der Patentfähigkeit  
in Betracht gezogene Druckschriften:

DE 43 33 474 A1  
DE 43 17 114 A1

⑤4 Verfahren zum Initialisieren eines Diebstahlschutzsystems für ein Kraftfahrzeug

⑤7 Für eine Wegfahrsperre mit mehreren tragbaren Transpondern  $T_i$  und einem Steuergerät 2 im Kraftfahrzeug sind eine vorbestimmte Anzahl von Freistarts erlaubt, ohne daß ein gültiges Codesignal empfangen werden muß. Sobald zwei Transponder  $T_i$  nacheinander das Steuergerät 2 aktivieren, wird das Diebstahlschutzsystem initialisiert. Freistarts sind dann nicht mehr möglich.





Die Erfindung betrifft ein Verfahren zum Initialisieren eines Diebstahlschutzsystems gemäß Oberbegriff von Patentanspruch 1.

Ein bekanntes Diebstahlschutzsystem (DE 43 33 474) weist mehrere tragbare Transponder auf, in denen jeweils codierte Daten gespeichert sind. Die Transponder sind auf einem Zündschlüssel angeordnet. Sobald der Zündschlüssel im Zündschloß verdreht wird, werden die codierten Daten des Transponders zu einem Steuergerät im Kraftfahrzeug übertragen. Wenn die übertragenen Daten mit Solldaten übereinstimmen, so wird ein Freigabesignal zum Starten des Motors erzeugt.

Damit die Transponder einem Steuergerät zugeordnet werden können, müssen sie zunächst initialisiert werden. Dies kann am Bandende beim Kraftfahrzeughersteller geschehen. Dabei werden erstmalig die codierten Daten in den Transponder eingeschrieben oder Daten des Transponders dem Steuergerät mitgeteilt.

Sobald der Zündschlüssel mit einem initialisierten Transponder in das Zündschloß eingesteckt und verdreht wird, erwartet das Steuergerät ein Codesignal des Transponders. Sobald das Steuergerät mit einer Spannung versorgt wird, erwartet es bereits ein Codesignal. Ohne dieses Codesignal sperrt das Steuergerät alle weiteren Vorgänge, wie Einschalten der Batteriespannung für Zusatzgeräte oder Funktionstests am Kraftfahrzeug.

Bei einem weiteren bekannten Diebstahlschutzsystem kann ein neuer Fahrzeugschlüssel mit einem zugeordneten Transpondercode dadurch initialisiert werden, in dem über ein manuelles Stellelement ein Initialisierungscode eingegeben wird. Wenn der neu eingegebene Initialisierungscode mit einem vorher in einem Speicher abgelegten Initialisierungscode übereinstimmt, so wird der Schlüssel als neuer berechtigter Schlüssel erkannt. Somit besteht die Möglichkeit, einen defekten Schlüssel zu ersetzen oder weitere Schlüssel für eine berechtigte Fahrzeugbenutzung zuzulassen.

Der Erfindung liegt das Problem zugrunde, ein Verfahren zum Initialisieren eines Diebstahlschutzsystems für ein Kraftfahrzeug zu schaffen, bei dem Funktionstests durchgeführt und alle zu dem Diebstahlschutzsystem zugeordneten Transponder initialisiert werden können.

Das Problem wird erfindungsgemäß durch die Merkmale des Patentanspruchs 1 gelöst.

Dabei wird eine vorbestimmte Anzahl von sogenannten Freistarts erlaubt. In dieser Zeit können Funktionstests an Armaturenbrett und Diebstahlschutzsystem durchgeführt werden, ohne daß dies Auswirkungen auf die Funktionstüchtigkeit hat. Der Motor kann ebenfalls gestartet werden, ohne daß ein Codesignal nötig ist. Sobald ein zweiter Transponder das Diebstahlschutzsystem aktiviert, wird dieses initialisiert. Danach ist nur noch ein Starten des Motors möglich, wenn ein oder mehrere korrekt initialisierte Transponder verwendet werden, die ihre Berechtigung durch ein Codesignal nachweisen.

Vorteilhafte Ausgestaltungen der Erfindung sind in den Unteransprüchen gekennzeichnet.

Ausführungsbeispiele der Erfindung werden anhand der schematischen Zeichnungen näher erläutert. Es zeigen:

Fig. 1 ein Blockschaltbild eines Diebstahlschutzsystems und

Fig. 2 ein Ablaufdiagramm eines erfindungsgemäßen Verfahrens zum Initialisieren des Diebstahlschutzsystems.

stems.

Ein Diebstahlschutzsystem weist mehrere tragbare Transponder  $T_i$  ( $i = 1$  bis  $n$ ) auf, die in ein Diebstahlschutzsystem, insbesondere eine Wegfahrsperre eines Kraftfahrzeugs, eingebunden sind. Ein Transponder  $T_i$  ist jeweils auf einem Schlüssel 1 oder auf einer Chipkarte angeordnet. In einem Speicher jedes Transponders  $T_i$  sind fahrzeugspezifische Daten abgespeichert mit deren Hilfe ein Codesignal erzeugt wird.

Sobald ein Transponder  $T_i$  aktiviert wird, sei es durch Einstecken des Schlüssels 1 in das Zündschloß, durch Einschalten der Stromversorgung des Kraftfahrzeugs oder durch Betätigen eines Schalters im Kraftfahrzeug, wird ein Codesignal zu einem Steuergerät 2 im Kraftfahrzeug übertragen. Das Steuergerät 2 empfängt das Codesignal über eine Antenne 3 und wertet es aus. Das Codesignal wird dabei mit einem Sollcodesignal verglichen. Bei Übereinstimmung der beiden wird ein Freigabesignal erzeugt, das zu einem Sicherheitsaggregat 4 im Kraftfahrzeug gesendet wird. Ein solches Sicherheitsaggregat 4 kann beispielsweise die Motorsteuerung oder sonstige Steuergeräte sein, die ein Starten des Motors nur bei nachgewiesener Berechtigung, d. h. bei Empfang des Freigabesignals, erlauben.

Nach der Herstellung des Kraftfahrzeugs sind Funktionstests beim Kraftfahrzeughersteller notwendig, durch die überprüft wird, ob alle gefertigten Teile ordnungsgemäß arbeiten. Hierzu muß der Schlüssel 1 in das Zündschloß gesteckt und verdreht werden. Hierbei wird zunächst die Fahrzeugbatteriespannung an diverse Geräte oder Anzeigeeinheiten im Armaturenbrett gelegt und danach die Zündung eingeschaltet. Da das Steuergerät 2 mit seiner Antenne 3 am Zündschloß angeordnet ist und bei Drehen des Zündschlüssels aktiviert wird (Aktivierungsvorgang), erwartet es ein Codesignal eines Transponders  $T_i$ . Erst wenn das Codesignal richtig empfangen wurde, kann der durch das Drehen des Zündschlüssels eingeleitete Vorgang beendet werden.

Damit diese Funktionstest ohne korrektes Codesignal durchgeführt werden können, ist erfindungsgemäß vorgesehen, daß eine vorbestimmte Anzahl von Aktivierungsvorgängen erlaubt sind (Freistart), bei denen kein Codesignal für das Steuergerät 2 erforderlich ist.

Aus Sicherheitsgründen darf jedoch die Anzahl von diesen sogenannten Freistarts nicht beliebig groß sein, weil ansonsten mit jedem Schlüssel 1 oder durch Kurzschließen der Zündung ein Starten des Motors ermöglicht wird. Im Normalbetrieb des Kraftfahrzeugs ist ein Starten des Motors jedoch nur durch Übertragen eines korrekten Codesignals möglich.

Damit die Transponder  $T_i$  einem Steuergerät 2 zugeordnet werden können, um eine korrekte Authentifikation zwischen Transponder  $T_i$  und Steuergerät 2 durchzuführen, müssen einerseits jedem Transponder  $T_i$  und/oder andererseits dem Steuergerät 2 vorbestimmte Daten eingeschrieben werden, die zum Erzeugen des Codesignals dienen (Initialisierung).

Die Transponder  $T_i$  können werkseitig bereits initialisiert sein, d. h. sie enthalten schon unterschiedliche, für jeden Transponder  $T_i$  spezifische Daten, wobei mehrere Transponder  $T_i$  einem Steuergerät 2 zugeordnet sind.

Ebenso benötigt das Steuergerät 2 entsprechende Daten, damit es zu jedem Codesignal von jeweils einem Transponder  $T_i$  ein gültiges Sollcodesignale einstellen und abspeichern kann.

Anhand der Fig. 2 wird das erfindungsgemäße Verfahren zum Initialisieren des Diebstahlschutzsystems erläutert. Sobald ein Aktivierungsvorgang vorgenommen

wird, d. h. z. B. die Spannungsversorgung des Steuergeräts 2 eingeschaltet wird, fordert das Steuergerät 2 ein Codesignal von einem Transponder  $T_1$  an.

In dem Steuergerät 2 ist ein Freistartzähler angeordnet, der die Anzahl der Aktivierungsvorgänge zählt. Sobald das Steuergerät 2 aktiviert wird, wird der Zählerstand des Freistartzählers um eins erhöht und mit einem Maximalwert verglichen. Solange der Zählerstand kleiner ist als der Maximalwert, ist ein Starten des Motors oder ein Funktionstest, in den das Steuergerät 2 eingebunden ist, möglich. Wenn der Zählerstand den Maximalwert überschritten hat, so wird kein Freistart mehr zugelassen. Aus Sicherheitsgründen findet dann auch keine Initialisierung statt.

Sobald ein korrektes Codesignal von einem Transponder  $T_1$  empfangen wurde, wird abgefragt, ob das Codesignal von einem ersten Transponder  $T_1$  oder von einem weiteren Transponder  $T_2$  oder  $T_3$  stammt. Wenn das Codesignal von dem ersten Transponder  $T_1$  stammt, so wird der Zählerstand des Freistartzählers mit dem Maximalwert verglichen und abhängig davon ein Freistart erlaubt oder nicht.

Wenn nach dem ersten Transponder  $T_1$  bereits der zweite Transponder  $T_2$  sein Codesignal zum Steuergerät 2 übertragen hat, so werden im folgenden alle Transponder  $T_i$ , die dem Diebstahlschutzsystem zugeordnet sind, und das Steuergerät 2 initialisiert.

Als Maximalwert können beispielsweise zehn Freistarts möglich sein. Somit wäre nach elf Aktivierungsvorgängen kein Freistart mehr möglich. Das Kraftfahrzeug kann danach nur noch mit Hilfe eines korrekt initialisierten Transponders  $T_1$  gestartet werden. Weitergehende Einschalt- und Ruhestromtests sind jedoch trotzdem mit einem Transponder  $T_i$  möglich, ohne daß eine Initialisierung erfolgt, solange nur der bislang verwendete Transponder  $T_1$  verwendet wird.

Bei einer Initialisierung werden diejenigen Daten, die zum Erzeugen des Codesignals notwendig sind, von dem Transponder  $T_1$  zu dem Steuergerät 2 oder von dem Steuergerät 2 zu dem Transponder  $T_i$  übertragen und dort abgespeichert. Das Steuergerät 2 kennt dann jeden einzelnen Transponder  $T_i$ , der dem Diebstahlschutzsystem zugeordnet ist und mit ihm dessen Sollcodesignal.

Die Codesignale aller Transponder  $T_i$  des Diebstahlschutzsystems können identisch sein oder sich beispielsweise nur durch eine Schlüsselnummer voneinander unterscheiden.

Sobald das Steuergerät 2 alle Daten empfangen hat, kann es auch Daten zurück zu den Transpondern  $T_i$  schicken, die die voreingestellten Daten der Transponder  $T_i$  überschreiben.

Falls bei der Initialisierung Daten in die Transponder  $T_i$  zurückgeschrieben werden, so kann dies für den ersten Transponder  $T_1$  dann geschehen, sobald er zum ersten Mal sein Codesignal abgibt oder nachdem der zweite Transponder  $T_2$  zum ersten Mal sein Codesignal ausgesendet hat.

Die Daten sind in Speichern jedes Transponders  $T_i$  und des Steuergeräts 2 gespeichert. Beispielsweise können hierzu  $E^2$  PROM-Bauelemente verwendet werden.

Mit diesem erfindungsgemäßen Verfahren zum Initialisieren des Diebstahlschutzsystems können Funktionstests im Kraftfahrzeug durchgeführt werden, ohne daß das System initialisiert ist. Allerdings wird nur eine vorbestimmte Anzahl von Freistarts, beispielsweise zehn Freistarts, erlaubt. Erst wenn ein Transponder  $T_i$  erkannt wird, der sich vom ersten Transponder  $T_1$  unterscheidet, beginnt der eigentliche Initialisierungsvor-

gang.

Ein Aktivierungsvorgang kann durch Einstecken des Schlüssels 1 in das Zündschloß oder durch Drehen des Schlüssels 1 im Zündschloß eingeleitet werden. Ein Aktivierungsvorgang kann auch durch Einschalten der Spannungsversorgung des Steuergeräts 2 oder durch Betätigen eines Zündschalters vorgenommen werden. Für die Erfindung ist es jedoch unwesentlich wie ein Aktivierungsvorgang vorgenommen wird. Wesentlich ist nur, daß eine vorbestimmte Anzahl von Aktivierungsvorgängen erlaubt ist, ohne daß das gesamte Diebstahlschutzsystem komplett initialisiert sein muß.

Sobald der zweite Transponder  $T_2$  einen Aktivierungsvorgang auslöst, beginnt die Initialisierung. Danach werden alle Transponder  $T_i$  innerhalb einer vorgegebenen Zeit, einer vorgegebenen Anzahl von Motorstarts oder in einer vorgegebenen Reihenfolge der Transponder  $T_i$  initialisiert. Dabei kann der erste Transponder  $T_1$  bereits bei seinem ersten Aktivierungsvorgang initialisiert worden sein, die restlichen Transponder  $T_2$  bis  $T_n$  werden nach dem zweiten Transponder  $T_2$  initialisiert.

Der Zählerstand des Freistartzählers wird nach der Initialisierung auf einen ungültigen Wert gesetzt, damit keine Freistarts mehr möglich sind. Nur noch mit einem korrekt arbeitenden Transponder  $T_i$ , der ein Codesignal zu dem Steuergerät 2 sendet, das mit einem Sollcodesignal übereinstimmt, kann ein Freigabesignal zum Starten des Motors erzeugt werden.

Die Daten, mit deren Hilfe das Sollcodesignal erzeugt wird, können fahrzeugspezifische Daten sein, die auf ein einziges Fahrzeug abgestimmt sind. Diese Daten sollten sich von denjenigen Daten unterscheiden, die für andere Kraftfahrzeuge bestimmt sind.

Mit dem erfindungsgemäßen Verfahren können die Fahrzeuge nach ihrer Herstellung gestartet und für die Überführung zu einem Händler bewegt werden. Die Schlüssel 1 mit den Transpondern  $T_i$  müssen somit auch nicht alle bereits bei der Fertigstellung des Fahrzeugs verfügbar sein, es genügt, wenn der Käufer alle Schlüssel 1 mit ihren Transpondern  $T_i$  beim Kauf des Kraftfahrzeugs erhält.

Bei der Erfindung ist ein Transponder  $T_i$  eine Vorrichtung, die ein Signal empfängt und daraufhin automatisch ein Antwortsignal aus sendet.

Bei einer Initialisierung werden zum ersten Mal diejenigen Daten festgelegt und gespeichert, die zum Erzeugen eines Codesignals notwendig sind, damit das Diebstahlschutzsystem korrekt arbeitet.

Die Codesignale werden drahtlos, beispielsweise induktiv, übertragen. Die Codesignale können bei jedem Aussenden gleich (Festcode) oder auch gemäß einer gespeicherten Rechenvorschrift bei jedem Aussenden verändert werden (Wechselcode).

#### Patentansprüche

1. Verfahren zum Initialisieren eines Diebstahlschutzsystems für ein Kraftfahrzeug, das aufweist:

- mehrere tragbare Transponder ( $T_i$ ), die jeweils einen Speicher zum Speichern von fahrzeugspezifischen Daten aufweisen,
- ein im Fahrzeug angeordnetes Steuergerät (2), das bei einem Aktivierungsvorgang einen Transponder ( $T_i$ ) auf fordert, Daten zu senden, diese Daten empfängt und mit Solldaten vergleicht sowie bei Übereinstimmung ein Freigabesignal zum Starten des Motors erzeugt, ge-

kennzeichnet durch folgende Schritte:

- daß das Freigabesignal automatisch innerhalb einer begrenzten Anzahl der Aktivierungsvorgänge unabhängig vom Empfang eines Codesignals jeweils erzeugt wird, 5
- daß in alle dem Diebstahlschutzsystem zugeordneten Transpondern ( $T_i$ ) neuen Daten oder/und in dem Steuergerät (2) neue Solldaten gespeichert werden, sobald ein zweiter Transponder ( $T_2$ ) einen Aktivierungsvorgang 10 auslöst, und
- daß dann ein Freigabesignal nur noch erzeugt wird, wenn die empfangenen Daten des jeweils verwendeten Transponders ( $T_i$ ) mit den jeweiligen Solldaten des Steuergeräts (2) 15 übereinstimmen.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß ein Aktivierungsvorgang durch Einstecken eines Zündschlüssels (1) in das Zündschloß oder Drehen des Zündschlüssels eingeleitet wird, 20 wobei ein Transponder ( $T_i$ ) auf dem Zündschlüssel angeordnet ist.

3. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß ein Aktivierungsvorgang durch Einschalten der Spannungsversorgung des Steuergeräts (2) eingeleitet wird. 25

4. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß ein Aktivierungsvorgang durch Betätigen eines Schalters eingeleitet wird.

5. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß die neuen Solldaten in das Steuergerät (2) oder neue Daten in weitere Transponder ( $T_i$ ) nur innerhalb einer vorgegebenen Zeit, bis zu einer vorgegebenen Anzahl von Motorstarts oder nur in einer vorgegebenen Reihenfolge der Transponder 30 ( $T_i$ ) eingeschrieben werden, sobald für den ersten Transponder ( $T_1$ ) neue Solldaten in das Steuergerät (2) oder neue Daten in den ersten Transponder ( $T_1$ ) eingeschrieben sind. 35

6. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß ein Freigabesignal nicht mehr erzeugt wird, wenn die begrenzte Anzahl von Aktivierungsvorgängen überschritten ist, ohne daß das Diebstahlschutzsystem initialisiert ist. 40

7. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß die Daten und die Solldaten fahrzeugspezifisch oder transponderspezifisch sind. 45

8. Diebstahlschutzsystem für ein Kraftfahrzeug, das mit einem Verfahren nach Anspruch 1 initialisiert ist. 50

---

Hierzu 2 Seite(n) Zeichnungen

---

55

60

65

FIG 1

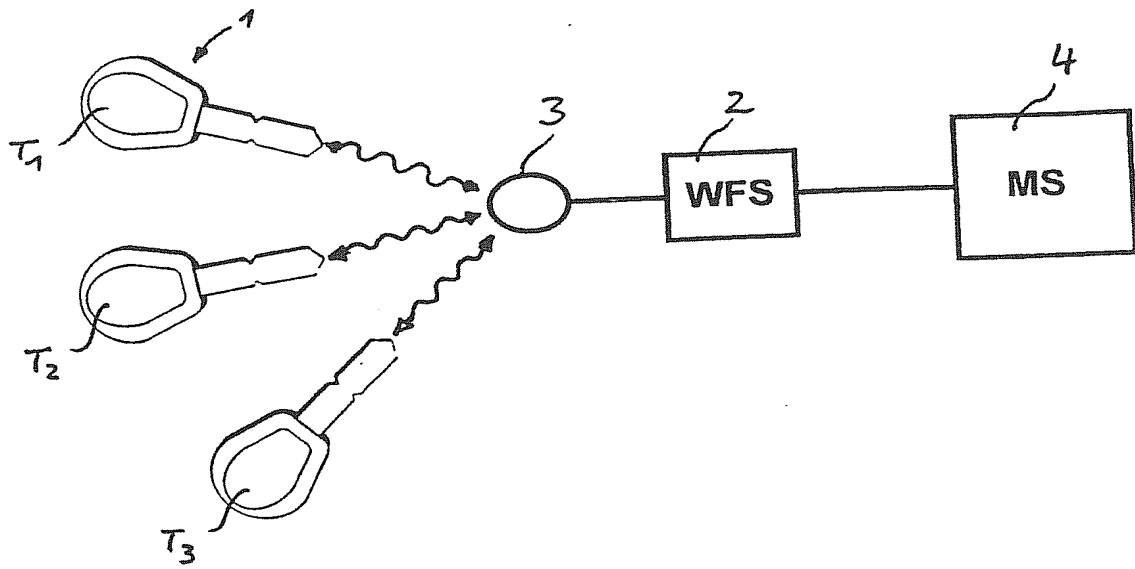


FIG 2

